Pushing Performance

People | Power | Partnership

HARTING Ha-VIS Management Software mCon 3000 Next Generation

User Manual Command Line Interface (CLI)

3rd Edition 2013, revised 10/13

© HARTING Electric GmbH & Co. KG, Espelkamp

Author: HARTING
Scriptor Dokumentations Service GmbH
Editor: HARTING

All rights reserved, including those of the translation.

No part of this manual may be reproduced in any form (print, photocopy, microfilm or any other process), processed, duplicated or distributed by means of electronic systems without the written permission of HARTING Electric GmbH & Co. KG, Espelkamp.

Subject to alterations without notice.

Printed on bleached cellulose. 100% free from chlorine and acid.

Content

1. Introduction 9
1.1 Purpose 9
1.2 Document Conventions 9
1.3 Key Conventions 9

2. Command Line Interface 10
2.1 CLI Command Modes 12

3. System Commands 14
3.1 Login 14
3.2 Help 14
3.3 Clear Screen 14
3.4 Enable 15
3.5 Disable 16
3.6 Configure Terminal 16
3.7 Configure 17
3.8 Listuser 17
3.9 Logout 18
3.10 End 19
3.11 Exit 20
3.12 Show Privilege 20
3.13 Show Users 21
3.14 Show History 21

4. System Features 22
4.1 Default Mode 22
4.2 Default IP Address 22
4.3 IP Address 23
4.4 IP Address DHCP 24
4.5 IP DHCP Client Discovery Timer 24
4.6 IP DHCP Client Fast-Access 24
4.7 IP DHCP Client Idle Timer 25
4.8 IP DHCP Snooping 25
4.9 Authorized-Manager IP-Source 26
4.10 IP HTTP Port 26
4.11 Feature Telnet 27
4.12 IP SSH 28
4.13 SSH Enable 31
4.14 Show IP SSH 31
4.15 IP SSH Transport-Max-Allowed Bytes 32
4.16 Interface 33
4.17 Write Startup-Config 34
4.18 Shutdown 35
4.19 System Contact 36
4.20 Clear Interfaces Counters 37
4.21 Clear Counters 37
4.22 Show IP Interface 38
4.23 Show Interfaces 39
4.24 Show Interfaces Counters 41
4.25 Show NVRAM 41
4.26 Show System Information 42
4.27 Show FlowControl 42
4.28 Show Running-Config 43
4.29 Show System Acknowledgement 44
4.30 FlowControl 45
4.31 Autonegotiation 46
4.32 Speed 47

4.33 Duplex 48
4.34 Autocrossing (MDI/MDIX) 49
4.35 SNMP Trap Link-Status 50

5. SNMPv3 51
5.1 SNMP User 51
5.2 SNMP Community Details 53
5.3 SNMP Engine ID 54
5.4 SNMP-Server Enable Traps 55
5.5 Show SNMP 56
5.6 Show SNMP Community 56
5.7 Show SNMP Engine ID 56
5.8 Show SNMP User 56
5.9 Show SNMP Server Traps 56

6. LLDP 57
6.1 Shutdown LLDP 57
6.2 Set LLDP 57
6.3 LLDP Transmit-Interval 58
6.4 LLDP Holdtime-Multiplier 59
6.5 LLDP Reinitialization-Delay 60
6.6 LLDP Tx-Delay 61
6.7 LLDP Notification-Interval 62
6.8 LLDP Chassis-ID-Subtype 63
6.9 Clear LLDP Counters 65
6.10 Clear LLDP Table 65
6.11 LLDP 66
6.12 LLDP Notification 67
6.13 LLDP TLV-Select Basic-TLV 69
6.14 LLDP Port-ID-Subtype 70
6.15 LLDP TLV-Select Dot1TLV 71
6.16 LLDP TLV-Select Dot3TLV 72
6.17 LLDP Dest-MAC 72
6.18 Show LLDP 73
6.19 Show LLDP Interface 73
6.20 Show LLDP Neighbors 74
6.21 Show LLDP Traffic 75
6.22 Show LLDP Local 76
6.23 Show LLDP Errors 76
6.24 Show LLDP Statistics 76

7. DHCP 77
7.1 Release DHCP 77
7.2 Renew DHCP 78
7.3 Show IP DHCP Client Stats 79
7.4 Service DHCP-Relay 79
7.5 IP DHCP Server 80
7.6 IP DHCP Relay Information Option 81
7.7 IP DHCP Relay Circuit-ID Option 82
7.8 IP DHCP Relay Circuit-ID 84
7.9 IP DHCP Relay Remote-ID 85
7.10 Show IP DHCP Relay Information 86
7.11 Show DHCP Server 87

8. (Rapid) Spanning Tree Protocol (RSTP, STP) 88
8.1 Shutdown Spanning-Tree 88
8.2 Spanning-Tree 89
8.3 Spanning-Tree ForwardTime/HelloTime/MaxAge 90
8.4 Spanning-Tree Transmit Hold-Count 92
8.5 Clear Spanning-Tree Counters 93
8.6 Spanning-Tree Pathcost Dynamic 94
8.7 Spanning-Tree Priority 96
8.8 Spanning-Tree Auto-Edge 97
8.9 Spanning-Tree Interface 98
8.10 Spanning-Tree Restricted-Role 100
8.11 Spanning-Tree Restricted-TCN 101
8.12 Spanning-Tree BDPU-Receive 102
8.13 Spanning-Tree BDPU-Transmit 103
8.14 Spanning-Tree Loop-Guard 104
8.15 Show Spanning-Tree Summary 105
8.16 Show Spanning-Tree Detail 106
8.17 Show Spanning-Tree Active 107
8.18 Show Spanning-Tree Interface 108
8.19 Show Spanning-Tree Root 110
8.20 Show Spanning-Tree Bridge 111

9. VLAN 112
9.1 Shutdown VLAN 112
9.2 VLAN 113
9.3 VLAN Learning Mode 114
9.4 Clear VLAN Statistics 114
9.5 Default VLAN ID 115
9.6 Ports 116
9.7 VLAN Active 119
9.8 Unicast-MAC Learning 120
9.9 Interface Range 121
9.10 Switchport Access VLAN 122
9.11 Switchport PVID 124
9.12 Switchport Ingress-Filter 126
9.13 Switchport Priority Default 127
9.14 Switchport Mode 128
9.15 VLAN Max-Traffic-Class 129
9.16 Show VLAN 130
9.17 Show VLAN Device Info 131
9.18 Show VLAN Device Capabilities 131
9.19 Show VLAN Traffic-Classes 132
9.20 Show VLAN Port Config 133
9.21 Show VLAN Protocol-Group 134

10. QoS / Diffserv 135
10.1 Shutdown QoS 135
10.2 QoS 136
10.3 QoS Scheduling Policy 137
10.4 QoS Match 138
10.5 QoS Override 139
10.6 QoS Tagifboth Match 140
10.7 Priority Map 141
10.8 Show QoS Global Info 141
10.9 Show Priority Map 141
10.10 Show Queue Map 142
10.11 Show QoS Port Configuration 142
10.12 Show QoS Port Override Configuration 142
10.13 Show QoS Scheduling Policy 143

11. Rate Limiting - Broadcast Storm Filter 144
11.1 Storm-Control 144
11.2 Rate-Limit Output 145

12. Port-Based Network Access Control (IEEE 802.1X) - PNAC 146
12.1 AAA Authentication Dot1x Default 146
12.2 Dot1x Local-Database 148
12.3 NAS-ID 149
12.4 Dot1x System-Auth-Control 149
12.5 Shutdown Dot1x 150
12.6 Dot1x Default 150
12.7 Dot1x Initialize 151
12.8 Dot1x Init-Session 151
12.9 Dot1x Max-Start 151
12.10 Dot1x Max-Req 152
12.11 Dot1x Reauthentication 153
12.12 Dot1x Init Session-Reauthentication 153
12.13 Dot1x Timeout 154
12.14 Dot1x Port-Control 157
12.15 Dot1x Access-Control 158
12.16 Dot1x Control-Direction 159
12.17 Dot1x Auth-Mode 160
12.18 Dot1x Host-Mode 161
12.19 Show Dot1x 162

13. RADIUS 164
13.1 RADIUS-Server Host 164
13.2 Show RADIUS Server 165
13.3 Show RADIUS Statistics 165

14. Link Aggregation (LA) 166
14.1 Set Port-Channel 166
14.2 Shutdown Port-Channel 167
14.3 Channel-Protocol 168
14.4 LACP System-Priority 169
14.5 LACP System-Identifier 170
14.6 LACP Port-Priority 171
14.7 LACP Port-Identifier 172
14.8 Channel-Group 173
14.9 LACP Wait-Time 175
14.10 LACP Timeout 176

14.11 LACP Rate 177
14.12 LACP Admin-Key 178
14.13 fault Port 179
14.14 Port-Channel Max-Ports 180
14.15 Show Etherchannel 181
14.16 Show Interfaces 183
14.17 Show LACP 184

15. IGMP 186
15.1 IP IGMP Snooping 186
15.2 IP IGMP Snooping Proxy-Reporting 187
15.3 Snooping Multicast-Forwarding-Mode 188
15.4 IP IGMP Snooping MRouter-Time-Out 189
15.5 IP IGMP Querier-Timeout 190
15.6 IP IGMP Snooping Port-Purge-Interval 191
15.7 IGMP Snooping Source-Only-Learning Age-Timer 192
15.8 IP IGMP Snooping Report-Suppression-Interval 193
15.9 IP IGMP Snooping Retry-Count 194
15.10 IP IGMP Snooping Group-Query-Interval 195
15.11 IP IGMP Snooping Report-Forwarding 196
15.12 IP IGMP Snooping Query-Forward 197
15.13 IP IGMP Snooping Version 198
15.14 IP IGMP Snooping Fast-Leave 199
15.15 IP IGMP Snooping VLAN Immediate-Leave 200
15.16 IP IGMP Snooping Querier 201
15.17 IP IGMP Snooping Querier-Interval 202
15.18 IP IGMP Snooping Startup-Querier-Interval 203
15.19 IP IGMP Snooping Startup-Querier-Count 204
15.20 IP IGMP Snooping Other-Querier-Present-Interval 205
15.21 IP IGMP Snooping MRouter 206
15.22 IP IGMP Snooping VLAN MRouter 207
15.23 Snooping Leave-Process Config-Level 208
15.24 IP IGMP Snooping Enhanced-Mode 209
15.25 IP IGMP Snooping Sparse-Mode 210
15.26 Snooping Report-Process Config-Level 211
15.27 Multicast VLAN Routing (MVR) 212
15.28 IP IGMP Snooping Filter 213
15.29 IP IGMP Snooping Blocked-Router 214
15.30 IP IGMP Snooping Leavemode 215
15.31 IP IGMP Snooping Ratelimit 216
15.32 IP IGMP Snooping Limit 217
15.33 IP IGMP Snooping Filter-ProfileID 218
15.34 IP IGMP Snooping Proxy 219
15.35 IP IGMP Snooping Max-Response-Code 220
15.36 IP IGMP Snooping MRouter-Port Purge Time-Out 221
15.37 IP IGMP Snooping MRouter-Port Version 222
15.38 Show IP IGMP Snooping MRouter 223
15.39 Show IP IGMP Snooping Globals 223
15.40 Show IP IGMP Snooping 224
15.41 Show IP IGMP Snooping Groups 225
15.42 Show IP IGMP Snooping Forwarding-Database 226
15.43 Show IP IGMP Snooping Statistics 227
15.44 Show IP IGMP Snooping Blocked-Router 227
15.45 Show IP IGMP Snooping Multicast-Receivers 228
15.46 Show IP IGMP Snooping Port-Cfg 228
15.47 IP IGMP Snooping Clear Counters 229
15.48 IP IGMP Snooping Send-Query 229
15.49 IP IGMP Snooping Static-Group 230

16. MAC-Address-Table 231
16.1 MAC-Address-Table Aging-Time 231
16.2 Show MAC-Address-Table 232
16.3 Show MAC-Address-Table Dynamic Unicast 233
16.4 Show MAC-Address-Table Dynamic Multicast 235
16.5 Show MAC-Address-Table Aging-Time 236

17. TCP 237
17.1 Show TCP Statistics 237
17.2 Show TCP Connections 237
17.3 Show TCP Listeners 237
17.4 Show TCP Retransmission Details 237

18. UDP 238
18.1 Show UDP Statistics 238
18.2 Show UDP Connections 238

1. Introduction

1.1 Purpose

This document describes in detail the CLI commands supported by HARTING switch software (hss). It is intended to be a reference manual for users and system administrators who will configure HARTING Ha-VIS mCon Switches through the CLI interface.

1.2 Document Conventions

- Elements in (< >) indicate the field required as input along with a CLI command, for example, < integer (100-1000)>.
- Elements in square brackets ([]) indicate optional fields for a command.
- Text in {} refers to either or group for the tokens given inside separated by a | symbol.
- The no form of the command resets a particular configuration to its default value or revokes the effect. This is explicitly explained in the description of the commands for which it is applicable.

1.3 Key Conventions

Keyboard shortcuts

Up Arrow/Down Arrow: Displays the previously executed command

Backspace/Ctrl-H: Removes a single character

TAB: Completes a command without typing the full word. If the command is not completely unique, it will be completed from the start to that position in the line where ambiguity begins. Now, you have to complete the rest of the command by yourself or press TAB again to get the help list with all possible commands. If there is no unique part inside your typing, the help list will be shown directly.

Left Arrow/Right Arrow: Traverses the current line

Others

?: Helps to list the available commands or show possible command completion

Example: show interfaces ?

q: Exits the output display if display is more than one page and returns to the hss prompt.

Show history: displays the command history list

2. Command Line Interface

This section describes the configuration of HSS using the Command Line Interface.

The Command Line Interface (CLI) can be used to configure the Intelligent Switch Solution from a console attached to the serial port of the switch or from a remote terminal using TELNET or SSH (depending on the installed features).

The HSS CLI supports a simple login authentication mechanism. The authentication is based on a user name and password provided by the user during login. The user “admin” is created by default with password “harting”.

If HSS is started, the user name and password has to be given at the login prompt to access the CLI shell. See example:

Harting Intelligent Switch Solution

Ha-VIS mCon 3102-AASFP login: admin

Password: *******

hss#

The “privileged-exec” mode is now available to the user admin. CLI Command Modes provide a detailed description of the various modes available for HSS.

The command prompt always displays the current mode.

- CLI commands need not be fully typed. The abbreviated forms of CLI commands are also accepted by the HSS CLI. For example, commands like “show ip interface” can be typed as “sh ip int”.
- CLI commands are case insensitive. For example, command “clear screen”, “CLEAR SCREEN” and “clEAr SCreen” are the same.
- CLI commands will be successful only if the dependencies are satisfied for a particular command that is issued. Appropriate error messages will be displayed, if the dependencies are not satisfied

Note

The Ethernet type of an interface is determined during System Startup. While configuring interface specific parameters, its Ethernet type needs to be specified correctly. A fast Ethernet interface cannot be configured as a gigabit Ethernet interface and vice-versa.

Example with Windows 7:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.
C:\>telnet 192.168.0.126
                Harting Intelligent Switch Solution
Ha-VIS mCon 3102-AASFP login: admin
Password: harting
hss#
hss#
hss# configure terminal
hss(config)#
hss(config)#
hss(config)# interface Gigabitethernet 0/1
hss(config-if)#
hss(config-if)#
hss(config-if)# exit
hss(config)#
hss(config)#
hss(config)# int Gi 0/1
hss(config-if)#
hss(config-if)#
hss(config-if)# exit
hss(config)#
hss(config)#
hss(config)# exit
hss#
hss#
hss# exit

Connection to Host Lost.

C:\>
```

2.1 CLI Command Modes

User EXEC Mode

After logging in to the device, the user is automatically in the User EXEC mode. In general, the User EXEC commands are used to temporarily change terminal settings, perform basic tests and list system information.

Command Mode	User EXEC
Access Method	This is the initial mode to start a session.
Prompt	hss>
Exit Method	The logout method is used.

Privileged EXEC Mode

Since many of the privileged commands set operating parameters, privileged access is password protected to prevent unauthorized use. The password is not displayed on the screen and is case sensitive. The Privileged EXEC mode prompt is the device name followed by the pound (#) sign.

Command Mode	Privileged EXEC
Access Method	The User EXEC mode command enable, is used to enter the Privileged EXEC mode.
Prompt	hss#
Exit Method	To return from the Privileged EXEC mode to User EXEC mode the disable command is used.

Global Configuration Mode

Global Configuration commands apply to features that affect the system as a whole, to any specific interface.

Command Mode	Global Configuration
Access Method	The Privileged EXEC mode command configure terminal, is used to enter the Global Configuration mode.
Prompt	hss(config)#
Exit Method	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.

Physical Interface Configuration Mode

The Physical Interface mode is used to perform interface specific operations. To return to the global configuration mode the exit command is used.

Command Mode	Interface Configuration
Access Method	The Global Configuration Mode command interface <interfacetype> <interfaceid> is used to enter the Interface configuration mode.
Prompt	hss(config-if)#
Exit Method	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.

Config-VLAN Mode

This mode is used to perform VLAN specific operations. To return to the global configuration mode the exit command is used.

Command Mode	Config-VLAN
Access Method	The global configuration mode command vlan <vlan-id>, is used to enter the Config-VLAN mode.
Prompt	hss(config-vlan)#
Exit Method	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.

MRP-Ring Configuration Mode

This mode is used to perform MRP Ring specific operations. To return to the global configuration mode the exit command is used.

Command Mode	MRP-Ring Configuration
Access Method	The global configuration mode command mrp ring <ring-id>, is used to enter the MRP-RingConfig mode.
Prompt	hss(Mrp-Ring)#
Exit Method	To exit to the Global Configuration mode the exit command is used and to exit to the Privileged EXEC mode the end command is used.

3. System Commands

3.1 Login

Command Description	Pre-Conditions	#	Step	Description	Result
Try to login to CLI	Telnet enabled on switch.	1	**Login with correct username and password**	Login with username: admin password: harting (Default value)	Login should be successful

3.2 Help

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays a brief description for the given command. help [command]	Mode: All Modes.	1	**help enable**	Help description for commands with one word, command name is **enable**.	Help description for command **enable** is displayed.
		2	**help en**	Input of incomplete command name **en**.	Help description for commands beginning with **en**.
		3	**help clearscreen**	Help description for commands with more than one word, command name is **clear screen**.	Help description for command clear **screen** is displayed.

3.3 Clear Screen

Command Description	Pre-Conditions	#	Step	Description	Result
This command clears all the contents from the screen. clear screen	Mode: All Modes.	1	**clear screen**	All content is cleared from the screen.	The screen is cleared.

3.4 Enable

Command Description	Pre-Conditions	#	Step	Description	Result
This command enters into default level privileged mode. If required, the user can specify the privilege level by enabling level with a password (login password) protection to avoid unauthorized use. enable [<0-15> Enable Level]	Mode: User EXEC Mode.	1	**enable**	Enter command enable and the password. System changes to Privileged EXEC Mode. Using the command **show privilege** that the privileged mode is turned on and privilege level is set to default value 15.	System is in Privileged EXEC Mode. Privilege level is 15.
		2	**enable 1**	Privilege level is 15. Enter command enable with privilege level 1. Using the command **show privilege** you can check if the privilege level is set to 1.	Privilege level is 1.
		3	**enable 15**	Privilege level is 1. Enter command enable with privilege level 15. Using the command **show privilege** you can check the privilege level is set to 15.	Privilege level is 15.

3.5 Disable

Command Description	Pre-Conditions	#	Step	Description	Result
This command turns off privileged commands. The privilege level varies between 0 and 15. This value should be less than the privilege level value given in the enable command. disable [<0-15> Privilege level to go to]	Mode: Privileged EXEC Mode.	1	**disable**	Privilege level: 15. Enter the command. System changes to User Mode. Using the command **show privilege** you can check if privilege level is set to 1.	System is in User EXEC Mode. Privilege level is 1.
		2	**disable 1**	Privilege level: 15. Enter the command. System changes to User Mode. Using the command **show privilege** you can check if privilege level is set to 1.	System is in User EXEC Mode. Privilege level is 1.
		4	**disable 15**	Privilege level: 15. Enter the command. Using the command **show privilege** you can check if privilege level stayed at 15.	System stayed in Privileged EXEC Mode. Privilege level stayed at 15.

3.6 Configure Terminal

Command Description	Pre-Conditions	#	Step	Description	Result
This command enters to Global Configuration Mode which allows the user to execute all the commands that support global configuration mode. configure terminal	Mode: Privileged EXEC Mode.	1	**configure terminal**	Mode: Privileged EXEC Mode. Enter the command. You can check if the Global Configuration Mode is turned on.	System is in Global Configuration Mode.
		2	**conf t**	Mode: Privileged EXEC Mode. Enter the command. You can check if the Global Configuration Mode is turned on.	System is in Global Configuration Mode.

3.7 Configure

Command Description	Pre-Conditions	#	Step	Description	Result
This command enters the configuration mode. It operates similar to the command configure terminal. configure	Mode: Privileged EXEC Mode	1	**configure**	Mode: Privileged EXEC Mode. Enter the command. You can check if the Global Configuration Mode is turned on.	System is in Global Configuration Mode.
		2	**conf**	Mode: Privileged EXEC Mode. Enter the command. You can check if the Global Configuration Mode is turned on.	System is in Global Configuration Mode.

3.8 Listuser

Command Description	Pre-Conditions	#	Step	Description	Result
This command lists all the default and newly created users, along with their permissible mode. listuser	Mode: Privileged EXEC Mode	1	**listuser**	Enter the command. You can check if default and newly created users with their permissible mode and privilege level are displayed.	Users are displayed.
		2	**listus**	Enter the command. You can check if default and newly created users with their permissible mode and privilege level are displayed.	Users are displayed.

3.9 Logout

Command Description	Pre-Conditions	#	Step	Description	Result
This command exits from Privileged EXEC / User EXEC mode and terminates the telnet session. logout	Mode: User EXEC Mode	1	**logout**	Mode: **User EXEC Mode.** Enter the command. The telnet session will be terminated.	Telnet session is terminated.
	Mode: Privileged EXEC Mode	2	**logout**	Mode: **Privileged EXEC Mode**. Enter the command. The telnet session will be terminated.	Telnet session is terminated.

3.10 End

Command Description	Pre-Conditions	#	Step	Description	Result
This command exits from the current mode to the Privileged EXEC mode. end	Mode: All Modes	1	**end**	Mode: **User EXEC Mode** Enter the command. System stays in User EXEC Mode.	System is in User EXEC Mode.
		2	**end**	Mode: **Privileged EXEC Mode**. Enter the command. System stays in Privileged EXEC Mode.	System is in Privileged EXEC Mode.
		3	**end**	Mode: **Global Configuration Mode**. Enter the command. System changes to Privileged EXEC Mode.	System is in Privileged EXEC Mode.
		4	**end**	Mode: **Interface Configuration Mode** (Physical). Enter the command. System changes to Privileged EXEC Mode.	System is in Privileged EXEC Mode.
		5	**end**	Mode: **Interface Configuration Mode** (Port). Enter the command. System changes to Privileged EXEC Mode.	System is in Privileged EXEC Mode.
		6	**end**	Mode: **Interface Configuration Mode** (VLAN). Enter the command. System changes to Privileged EXEC Mode.	System is in Privileged EXEC Mode.
		7	**end**	Mode: **Config-VLAN Mode**. Enter the command. System changes to Privileged EXEC Mode.	System is in Privileged EXEC Mode.
		8	**end**	Mode: **MRP-Ring Configuration Mode**. Enter the command. System changes to Privileged EXEC Mode.	System is in Privileged EXEC Mode.

3.11 Exit

Command Description	Pre-Conditions	#	Step	Description	Result
This command exits from the current configuration mode. exit	Mode: All Modes	1	**exit**	Mode: **Global Configuration Mode**. Enter the command. System changes to Privileged Mode.	System is in Privileged Mode.
		2	**exit**	Mode: **Interface Configuration Mode** (Physical). Enter the command. System changes to Global Configuration Mode.	System is in Global Configuration Mode.
		3	**exit**	Mode: **Interface Configuration Mode** (VLAN). Enter the command. System changes to Global Configuration Mode.	System is in Global Configuration Mode.
		4	**exit**	Mode: **Interface Configuration Mode** (Port-Channel). Enter the command. System changes to Global Configuration Mode.	System is in Global Configuration Mode.
		5	**exit**	Mode: **Config-VLAN Mode**. Enter the command. System changes to Global Configuration Mode.	System is in Global Configuration Mode.
		6	**exit**	Mode: MRP-Ring Configuration Mode. Enter the command. System changes to Global Configuration Mode.	System is in Global Configuration Mode.

3.12 Show Privilege

Command Description	Pre-Conditions	#	Step	Description	Result
This command shows the current user privilege level. show privilege	Mode: Privileged EXEC Mode or User EXEC Mode	1	**show privilege**	Enter the command. You can check if the current privilege level is displayed.	Current privilege level is displayed.

3.13 Show Users

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the information about the current user. show users	Mode: Privileged EXEC Mode	1	**show users**	Enter the command. Information about the current users are displayed.	Line, name and peer-address information about the current users are displayed.

3.14 Show History

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays a list of recently executed commands. show history	Mode: Privileged EXEC Mode	1	**show history**	Enter the command. The recently executed commands are listed.	The recently executed commands are listed.

4. System Features

4.1 Default Mode

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the mode by which the default interface gets its IP address. This configuration takes effect only on switch restart. default mode { manual | dynamic } Hint: 'Manual' is the default value.	Mode: Global Config Mode	1	**default mode dynamic**	Default IP Address Config Mode: **Manual** Enter the command. Using the command **show nvram** in Privileged EXEC Mode you can check if Default IP Address Config Mode is set to **Dynamic**.	Default IP Address Config Mode: Dynamic
		2	**default mode manual**	Default IP Address Config Mode: **Dynamic** Enter the command. Using the command **show nvram** in Privileged EXEC Mode you can check if Default IP Address Config Mode is set to **Manual**. Hint: Manual is the default value.	Default IP Address Config Mode: Manual

4.2 Default IP Address

Command Description	Pre-Conditions	#	Step	Description	Result
Configures the IP address and subnet mask for the default interface. default ip address <ip-address> [subnet-mask <subnet mask>] [interface <interface-type> <interface-id>]	Mode: Global Config Mode	1	**default ip address 20.0.0.1 subnet-mask 255.0.0.0**	Sets the default IP address to 20.0.0.1, with a subnet mask of 255.0.0.0.	show nvram should show the configured default IP address.

4.3 IP Address

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the IP address for an interface. The no form of the command resets the IP address of the interface to its default value. ip address <ip-address> <subnet-mask> [secondary] no ip address [<ip_addr>] Hint: 192.168.0.126 255.255.255.0 is the default value.	Mode: Interface Config Mode (VLAN Interface Mode)	1	**ip address 192.168.1.128 255.255.255.0**	The interface is shut down. Enter the command. Using the command **show ip interface** you can check if interface address is set to 192.168.1.128.	Interface address is 192.168.1.128.
		2	**ip address 192.168.1.129 255.255.255.0 secondary**	The interface is shut down. Primary address is configured. Enter the command. Using the command **show ip interface** you can check if secondary address is set to 192.168.1.129.	Secondary address is 192.168.1.129.
		3	**no ip address 192.168.1.129 255.255.255.0 secondary**	The interface is shut down. Enter the command. Using the command **show ip interface** you can check if secondary address is deleted.	Secondary address 192.168.1.129 is deleted.
		4	**no ip address 192.168.1.128 255.255.255.0**	The interface is shut down. Secondary address is deleted. Enter the command. Using the command **show ip interface** you can check if interface address is deleted.	Interface address 192.168.1.128 is deleted and set to 0.0.0.0.

4.4 IP Address DHCP

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the current VLAN / OOB interface to dynamically acquire an IP address from the RARP / DHCP server. The no form of the command resets the IP address for the interface to its default value. ip address { dhcp | rarp } [client-id { FastEthernet | GigabitEthernet | Portchannel | Vlan } <interface_list>] [hostname <host_name>]	Mode: Interface Config Mode (VLAN)	1	**ip address dhcp**	Try to make a DHCP request for the interface.	**show ip dhcp client stats** should show the acquired address.

4.5 IP DHCP Client Discovery Timer

Command Description	Pre-Conditions	#	Step	Description	Result
Configure DHCP Client Discovery Timer. Seconds to wait between discovery messages sent by DHCP client. The no form of the command resets the IP address for the interface to its default value. ip dhcp client discovery timer <integer (1-9)> no ip dhcp client discovery timer	Mode: Privileged EXEC Mode	1	**ip dhcp client discovery timer 5**	Set the timer to five seconds.	**show ip dhcp client stats** should show the configured discovery timer.

4.6 IP DHCP Client Fast-Access

Command Description	Pre-Conditions	#	Step	Description	Result
Enables DHCP client fast access mode. The no form of the command resets the IP address for the interface to its default value. ip dhcp client fast-access no ip dhcp client fast-access	Mode: Privileged EXEC Mode	1	**ip dhcp client fast-access**	Enables DHCP client fast access mode.	**show ip dhcp client fast-access** should show that fast-access mode is enabled.

4.7 IP DHCP Client Idle Timer

Command Description	Pre-Conditions	#	Step	Description	Result
Configure DHCP Client Idle Timer. Seconds to wait after four unsuccessful DHCP client discovery messages. The no form of the command resets the IP address for the interface to its default value. ip dhcp client idle timer <integer (1-30)> no ip dhcp client idle timer	Mode: Privileged EXEC Mode	1	**ip dhcp client idle timer 10**	Set the idle timeout to 10 seconds.	**show ip dhcp client fast-access** should show the configured timeout value.

4.8 IP DHCP Snooping

Command Description	Pre-Conditions	#	Step	Description	Result
Enables Layer 2 DHCP Snooping in the VLAN. The no form of the command disables the function. ip dhcp snooping no ip dhcp snooping	Mode: VLAN Config Mode	1	**ip dhcp snooping**	Enable Layer 2 DHCP Snooping in the VLAN.	**show ip dhcp snooping vlan X** should show that DHCP snooping is enabled for VLAN X.

4.9 Authorized-Manager IP-Source

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures an IP authorized manager and the no form of the command removes manager from authorized managers list. authorized-manager ip-source <ip-address> [{<subnet-mask> | / <prefix-length(0-32)>}] [interface [<interface-type <0/a-b, 0/c, ...>] [<interface-type <0/a-b, 0/c, ...>] <interface-type <a,b or a-b or a,b,c-d...>]] [vlan <a,b or a-b or a,b,c-d>] [cpu0] [service [snmp] [telnet] [http] [https] [ssh]] channel-protocol { lacp | pagp } no authorized-manager ip-source < ip-address > [{ <subnet-mask > | / <prefixlength(1-32)> }]	Mode: Global Config Mode	1	**authorized-manager ip-source 10.203.113.5 255.255.255.255 interface gigabitethernet 0/1 vlan 1 service snmp**	Authorize the host with IP 10.203.113.5 and subnet mask 255.255.255.0, connected to gigabit Ethernet 0/1 interface in vlan 1 to configure the switch via SNMP.	The switch can now be configured via snmp from the specified host.

4.10 IP HTTP Port

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the HTTP port. This port is used to configure the router using the Web interface. The value ranges between 1 and 65535. The no form of the command resets the HTTP port to its default value. ip http port <port(1-65535)> no ip http port Hint: Default value is 80.	Mode: Global Config Mode	1	**ip http port 90**	HTTP-Port: 80 Enter the command. You can check if HTTP-Port is set to 90.	HTTP-Port: 90
		2	**no ip http port**	HTTP-Port: 90 Enter the command. You can check if HTTP-Port is set to default value 80.	HTTP-Port: 80

4.11 Feature Telnet

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the telnet service in the system. The no form of this command disables the telnet service. feature telnet no feature telnet	Mode: Global Config Mode	1	**no feature telnet**	Telnet service is enabled. Enter the command.	Telnet session is terminated. A re-login is not possible, because the telnet service is disabled.

4.12 IP SSH

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the various parameters associated with SSH server. The no form of this command re-sets the various parameters associated with SSH server. The standard port used by SSH is 22. SSH server allows remote and secure configuration of the switch. The SSH server provides protocol version exchange, data integrity, cipher and key exchange algorithms negotiation between two communicating entities, key exchange mechanism, encryption and server authentication. The auth takes values as bit mask. Setting a bit indicates that the corresponding MAC-list will be used for authentication. ip ssh { version compatibility | cipher ([des-cbc] [3des-cbc] [aes128-cbc] [aes256-cbc]) | auth ([hmac-md5] [hmac-sha1]) } no ip ssh { version compatibility | cipher ([des-cbc] [3des-cbc] [aes128-cbc] [aes256-cbc]) | auth ([hmac-md5] [hmac-sha1]) }	Mode: Global Config Mode	1	**ip ssh version compatibility**	Version of the SSH is 2. Enter the command. Using the command **show ip ssh** you can check if version of the SSH is set to both.	Version of the SSH is both.
		2	**no ip ssh version compatibility**	Version of the SSH is both. Enter the command. Using the command **show ip ssh** you can check if version of the SSH is set to 2.	Version of the SSH is 2.
		3	**ip ssh cipher des-cbc**	Cipher Algorithm is 3DES-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to DES-CBC.	Cipher Algorithm is DES-CBC.

Command Description	Pre-Conditions	#	Step	Description	Result
		4	**ip ssh cipher 3des-cbc**	Cipher Algorithm is DES-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to 3DES-CBC.	Cipher Algorithm is 3DES-CBC.
		5	**ip ssh cipher aes128-cbc**	Cipher Algorithm is 3DES-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to AES128-CBC.	Cipher Algorithm is AES128-CBC.
		6	**ip ssh cipher aes256-cbc**	Cipher Algorithm is 3DES-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to AES256-CBC.	Cipher Algorithm is AES256-CBC.
		7	**ip ssh cipher des-cbc 3des-cbc aes128-cbc aes256-cbc**	Cipher Algorithm is 3DES-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to DES-CBC, 3DES-CBC, AES128-CBC, AES256-CBC.	Cipher Algorithm is DES-CBC, 3DES-CBC, AES128-CBC, AES256-CBC.
		8	**no ip ssh cipher aes256-cbc**	Cipher Algorithm is DES-CBC, 3DES-CBC, AES128-CBC, AES256-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to DES-CBC, 3DES-CBC, AES128-CBC.	Cipher Algorithm is DES-CBC, 3DES-CBC, AES128-CBC.

Command Description	Pre-Conditions	#	Step	Description	Result
		9	**no ip ssh cipher aes128-cbc**	Cipher Algorithm is DES-CBC, 3DES-CBC, AES128-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to DES-CBC, 3DES-CBC.	Cipher Algorithm is DES-CBC, 3DES-CBC.
		10	**no ip ssh cipher 3des-cbc**	Cipher Algorithm is DES-CBC, 3DES-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to DES-CBC.	Cipher Algorithm is DES-CBC.
		11	**no ip ssh cipher des-cbc**	Cipher Algorithm is DES-CBC, 3DES-CBC. Enter the command. Using the command **show ip ssh** you can check if Cipher Algorithm is set to 3DES-CBC.	Cipher Algorithm is 3DES-CBC.
		12	**ip ssh auth hmac-md5**	Authentication is HMAC-SHA1. Enter the command. Using the command **show ip ssh** that Authentication is set to HMAC-MD5.	Authentication is HMAC-MD5.
		13	**ip ssh auth hmac-sha1**	Authentication is HMAC-MD5. Enter the command. Using the command show ip ssh you can check if Authentication is set to HMAC-SHA1.	Authentication is HMAC-SHA1.
		14	**no ip ssh auth hmac-md5**	Authentication is HMAC-MD5. Enter the command. Using the command **show ip ssh** you can check if Authentication is set to HMAC-SHA1.	Authentication is HMAC-SHA1.

4.13 SSH Enable

Command Description	Pre-Conditions	#	Step	Description	Result
This command either enables or disables the SSH subsystem. If set to enable, the switch is accessible through SSH from a remote locations. Setting SSH to disable, removes the SSH access to the switch. ssh { enable | disable }	Mode: Global Config Mode	1	**ssh disable**	SSH subsystem is enabled. Enter the command. You can check if the SSH subsystem is disabled.	SSH is disabled.
		2	**ssh enable**	SSH subsystem is disabled. Version: Both. Cipher Algorithm: 3DES-CBC, DES-CBC, AES128-CBC, AES256-CBC. Authentication: HMAC-MD5. Enter the command. Using the command **show ip ssh** you can check if SSH parameters are set to default values: Version: 2. Cipher Algorithm: 3DES-CBC Authentication: HMAC-SHA1.	SSH is enabled.

4.14 Show IP SSH

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the SSH server information such as version, cipher algorithm, authentication and trace level. show ip ssh	Mode: Privileged EXEC Mode	1	**show ip ssh**	Enter the command. You can check if SSH server information such as version, cipher algorithm, authentication and trace level is displayed.	SSH is disabled.

4.15 IP SSH Transport-Max-Allowed Bytes

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the maximum number of bytes allowed in an SSH transport connection. The maximum allowed bytes ranges between 1 and 32768. The SSH connection will be allowed only if the packet size does not exceed the value configured and is dropped if the value exceeds the configured. ip ssh transport-max-allowed bytes <integer(1-32768)>	Mode: Global Config Mode	1	**ip ssh transport-max-allowed bytes 1**	Max Byte Allowed: 32768. Enter the command. Using the command **show ip ssh** you can check if Max Byte Allowed is set to 1.	Max Byte Allowed is 1.
		2	**ip ssh transport-max-allowed bytes 2000**	Max Byte Allowed: 1. Enter the command. Using the command **show ip ssh** you can check if Max Byte Allowed is set to 2000.	
		3	**ip ssh transport-max-allowed bytes 32768**		
		4	**ip ssh transport-max-allowed bytes 0**		
		5	**ip ssh transport-max-allowed bytes 32769**		

4.16 Interface

Command Description	Pre-Conditions	#	Step	Description	Result
This command allows to configure interfaces. The no form of the command deletes interface such as VLAN, port channel, tunnel interface and so on. interface { cpu0 | vlan <vlan-id (1-4094)> [switch <switch-name>] | port-channel <port-channel-id (1-65535)> | tunnel <tunnel-id (0-128)> | <interface-type> <interface-id> | linuxvlan <interface-name> | loopback <interface-id (0-100)> | ppp <1-10> | pw <interface-id (1-65535)>| sisp <interface-id (1-65535)>| virtual <integer (1-16777214)>| mplstunnel <tunnel-id (1-65535)> } no interface { vlan <vlan-id (1-4094)> [switch <switch-name>] | port-channel <port-channel-id(1-65535)> | tunnel <tunnel-id (0-128)> | <interface-type> <interface-id> | linuxvlan <interface-name> | loopback <interface-id (0-100)> | ppp <integer (1-10)> | pw <integer (1-65535)| sisp <interface-id(1-65535)>| virtual <integer (1-16777214)> | mplstunnel <tunnel-id (1-65535)> [gracefuldeletion }	Mode: Global Config Mode	1	**interface vlan 2**	Enter the command. The system changes to Interface Configuration Mode (VLAN).	The system is in Interface Configuration Mode (VLAN).
		2	**interface port-channel 10**	Enter the command. The system changes to Interface Configuration Mode (Port-channel).	The system is in Interface Configuration Mode (Port-channel).
		3	**interface tunnel 1**	Enter the command. The system changes to Interface Configuration Mode (Tunnel).	The system is in Interface Configuration Mode (Tunnel).
		4	**interface loopback 1**	Enter the command. The system changes to Interface Configuration Mode (Loopback).	The system is in Interface Configuration Mode (Loopback).

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**no interface vlan 2**	Vlan 2 exists. Enter the command. Using the command show interfaces you can check if interface vlan 2 is deleted.	Interface vlan 2 is deleted.
		6	**no interface port-channel 10**	Port-channel 10 exists. Enter the command. Using the command show interfaces you can check if interface Port Channel 10 is deleted.	Interface Port Channel 10 is deleted.

4.17 Write Startup-Config

Command Description	Pre-Conditions	#	Step	Description	Result
This command writes the running-config to a flash file, startup-configuration file or to a remote site. write { flash:filename | startup-config | tftp://ip-address/filename | sftp://<user-name>:<password>@ip-address/filename }	Mode: Privileged EXEC Mode	1	**write startup-config**	Enter the command write startup-config. The actual running configuration is copied from the memory to the flash memory into the startup configuration.	Configuration is saved persistent.
		2	**ip ssh transport-max-allowed bytes 2000**	Max Byte Allowed: 1. Enter the command. Using the command **show ip ssh** you can check if Max Byte Allowed is set to 2000.	
		3	**ip ssh transport-max-allowed bytes 32768**		
		4	**ip ssh transport-max-allowed bytes 0**		
		5	**ip ssh transport-max-allowed bytes 32769**		

4.18 Shutdown

Command Description	Pre-Conditions	#	Step	Description	Result
This command disables a physical interface / VLAN interface / port channel interface / tunnel interface / OOB interface. The no form of the command enables a physical interface / VLAN interface / port channel interface / tunnel interface / OOB interface. shutdown no shutdown	Mode: Interface Config Mode for physical interface / port – channel / tunnel interface / OOB Interface, VLAN Interface Mode for VLAN interface	1	**shutdown**	Interface Configuration Mode (Port-Channel). Port Channel 1 is selected and not shut down. Enter the command. Using the command show interfaces you can check if Port Channel is shut down.	Port Channel 1 is shutdown.
		2	**no shutdown**	Interface Configuration Mode (Port-Channel). Port Channel 1 is selected and shut down. Enter the command. Using the command show interfaces you can check if Port Channel is not shut down.	Port Channel 1 is not shutdown.
		3	**shutdown**	Interface Configuration Mode (Physical). Gi0/1 is selected and not shut down. Enter the command. Using the command show interfaces you can check if port is shut down.	Port Gi0/1 is shutdown.
		4	**no shutdown**	Interface Configuration Mode (Physical). Gi0/1 is selected and shut down. Enter the command. Using the command show interfaces you can check if port is not shut down.	Port Gi0/1 is not shutdown.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**shutdown**	Interface Configuration Mode (VLAN). VLAN 2 is selected and not shut down. Enter the command. Using the command show interfaces you can check if VLAN 2 is shut down.	VLAN 2 is shutdown.
		6	**no shutdown**	Interface Configuration Mode (VLAN). VLAN 2 is selected and shut down. Enter the command. Using the command show interfaces you can check if VLAN 2 is not shut down.	VLAN 2 is not shutdown.

4.19 System Contact

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the system contact information. system contact <contact info>	Mode: Global Config Mode	1	**system contact "HARTING Electric"**	System Contact is "Harting ICPN" per default. Enter the command. Using the command show system information you can check if System Contact is set to new value.	System Contact is set to: HARTING Electric.

4.20 Clear Interfaces Counters

Command Description	Pre-Conditions	#	Step	Description	Result
This command clears all the current interface counters from the interface unless the optional arguments type and number are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on). clear interfaces [<interface-type> <interface-id>] counters	Mode: Global Config Mode	1	**system contact "HARTING Electric"**	System Contact is "Harting ICPN" per default. Enter the command. Using the command show system information you can check if System Contact is set to new value.	System Contact is set to: HARTING Electric.

4.21 Clear Counters

Command Description	Pre-Conditions	#	Step	Description	Result
This command clears all the current interface counters from the interface unless the optional arguments type and number are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on). This command is a standardized implementation of the existing command and operates similar to that of the command clear interfaces - counters. clear counters [<interface-type> <interface-id>]	Mode: Privileged EXEC Mode	1	**clear counters**	Enter the command. Using the command **show interfaces counters** you can check if all current interface counters are cleared.	All current interface counters are cleared.
		2	**clear counters gigabitethernet 0/5**	Enter the command. Using the command **show interfaces counters** you can check if counters for port Gi0/5 are cleared.	Counters for port Gi 0/5 are cleared.

4.22 Show IP Interface

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the IP interface configuration. show ip interface loopback <loopback-id(0-100)> show ip interface [vrf <vrf-name>] [Vlan <vlan-id(1-4094)> [switch <switchname>]] [<interface-type><interface-id>] [loopback <loopback-id(0-100)>]	Mode: Privileged EXEC Mode	1	**show ip interface**	Enter the command.	IP interface configuration for all available interfaces is displayed.
		2	**show ip interface gigabitethernet 0/1**	Enter the command.	IP interface configuration for Gigabitethernet 0/1 is displayed.
		3	**show ip interface vlan 1**	Enter the command.	IP interface configuration for the VLAN with ID=1 is displayed.

4.23 Show Interfaces

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the interface status and configuration. show interfaces [{ [<interface-type> <interface-id>] [{ description | stormcontrol | flowcontrol | capabilities | status | port-security-state }] | { vlan <vlan-id(1-4094)> [{ switch <switch-name> }] } | port-channel <port-channelid (1-65535)> | tunnel <tunnel-id (0-128)> } | private-vlan mapping }]	Mode: Privileged EXEC Mode	1	**show interfaces**	Enter the command.	Interface status and configuration for all available interfaces are displayed.
		2	**show interfaces gigabitethernet 0/1**	Enter the command.	Interface status and configuration for gigabitethernet interface (Gi0/1) are displayed.
		3	**show interfaces description**	Enter the command.	Admin status and protocol status for all available interfaces are displayed.
		4	**show interfaces storm-control**	Storm control is enabled for all interfaces. Enter the command.	Storm control information (storm control type and storm control limit) for all interfaces is displayed.
		5	**show interfaces flowcontrol**	Enter the command.	Flow control related statistics information for all interfaces is displayed.
		6	**show interfaces capabilities**	Enter the command.	Interface type, interface speed, duplex operation and flowcontrol status for the interfaces are displayed.
		7	**show interfaces status**	Enter the command.	The status, duplex details, speed and negotiation mode for the interfaces are displayed.

Command Description	Pre-Conditions	#	Step	Description	Result
		8	**show interfaces port-security-state**	Enter the command.	The state of the port security option for the interfaces is displayed.
		9	**show interfaces vlan 1**	Enter the command.	Interface status and configuration for the VLAN with ID=1 are displayed. Hint: VLAN1 is always configured.
		10	**show interfaces port-channel 11**	Port Channel with ID=11 is configured. Enter the command.	Interface status and configuration for the Port Channel with ID=11 are displayed. Hint: First Link-Aggregation is configured as Port Channel 11.

4.24 Show Interfaces Counters

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the interface statistics for each port. show interfaces [{ <interface-type> <interface-id> | vlan < short(1-4094)> [switch <switch-name>] | tunnel <tunnel-id(0-128)> | ppp <short(1-4094)> | HC }] counters	Mode: Privileged EXEC Mode	1	**show interfaces counters**	Enter the command.	Interface incoming and outgoing traffic statistics for all interfaces are displayed.
		2	**show interfaces gigabitethernet 0/1 counters**	Enter the command.	Interface incoming and outgoing traffic statistics for the gigabitethernet 0/1 are displayed.
		3	**show interfaces vlan 1 counters**	Enter the command.	Interface incoming and outgoing traffic statistics for the VLAN 1 are displayed.
		4	**show interfaces port-channel 1 counters**	Port-channel 1 is configured. Enter the command.	Interface incoming and outgoing traffic statistics for the Port Channel 1 are displayed.

4.25 Show NVRAM

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the current information stored in the NVRAM. show nvram	Mode: Privileged EXEC Mode	1	**show nvram**	Enter the command.	The information stored in the NVRAM is displayed.

4.26 Show System Information

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays system information. show system information	Mode: Privileged EXEC Mode	1	**show system information**	Enter the command. Check if the system information is displayed.	The system information is displayed.

4.27 Show FlowControl

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the flow-control information. show flow-control [interface <interface-type> <interface-id>]	Mode: Privileged EXEC Mode	1	**show flow-control**	Enter the command.	Flow-control information for all interfaces is displayed.
		2	**show flow-control interface gigabitethernet 0/1**	Enter the command.	Flow-control information for the gigabitethernet 0/1 is displayed.
		3	**show flow-control interface port-channel 1**	Port-channel 1 is configured. Enter the command.	Flow-control information for the Port Channel 1 is displayed.

4.28 Show Running-Config

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the configuration information currently running on the router, the configuration for a specific interface, or map class information. The configuration is lost if the system is restarted. Given, if the command is useful for looking at the configuration of a specific interface (provided that there are multiple interfaces). show running-config [{ dhcp | qos | stp [switch <context_ name>] | la | pnac | vlan <vlan-id(1-4094)> [switch <context_name>] | interface { port-channel <port-channel-id(1-65535)> | <interfacetype> <interfacenum> | vlan <vlan-id(1- 4094)> } | ssh | ssl | acl | ip | snmp | radius | rmon | rm | mbsm | igmp | igmp-proxy | sntp | switch <context_name> | [switch <context_name>] | entity-mib | http | ptp | lldp | system }]	Privileged EXEC Mode	1	**show running-config**	Enter the command.	Current active configurations are displayed.

4.29 Show System Acknowledgement

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays acknowledgement statement for open sources used in the software. show system acknowledgement	Mode: Privileged EXEC Mode	1	**show system acknowledgement**	Enter the command.	Acknowledgement statement for open sources used in the software is displayed.

4.30 FlowControl

Command Description	Pre-Conditions	#	Step	Description	Result
This command is used to set the send or receive flow-control value for an interface. If flowcontrol send is on for a device and any congestion is detected, it notifies the link partner or the remote device of the congestion by sending a pause frame. If flowcontrol receive is on for the remote device and it receives a pause frame, it stops sending any data packets. This prevents any loss of data packets during the congestion period. PAUSE is a flowcontrol mechanism that is implied on full duplex Ethernet link segments. The mechanism uses MAC control frames to carry the PAUSE commands. flowcontrol { on | off }	Interface Config Mode (Gigabitethernet interface or Port Channel)	1	**flowcontrol on**	Interface is selected and shut down. Enter the command. Using the command **show flow-control** you can check if flow control is set to ON (Admin Tx ON, Admin Rx ON).	Flow control is set to ON (Admin Tx ON, Admin Rx ON).
		2	**flowcontrol off**	Interface is selected and shut down. Enter the command. Using the command **show flow-control** you can check if flow control is set to OFF (Admin Tx OFF, Admin Rx OFF).	Flow control is set to OFF (Admin Tx OFF, Admin Rx OFF).

4.31 Autonegotiation

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the auto-negotiation of the interface. negotiation	Mode: Interface Config Mode (Gigabitethernet interface)	1	**negotiation**	Interface is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the auto-negotiation of the interface is enabled.	Auto-negotiation of the interface is enabled.
		2	**no negotiation**	Interface is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the auto- negotiation of the interface is disabled.	Auto-negotiation of the interface is disabled.

4.32 Speed

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the speed of the interface. speed { 10 | 100 | 1000 | auto | nonegotiate }	Mode: Interface Config Mode (Gigabitethernet interface)	1	**speed 10**	Interface is selected. Autonegotiation is disabled. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the speed of the interface is set to 10 Mbit/s.	Speed of the interface is 10 Mbit/s.
		2	**speed 100**	Interface is selected. Autonegotiation is disabled. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the speed of the interface is set to 100 Mbit/s.	Speed of the interface is 100 Mbit/s.
		3	**speed 1000**	Interface is selected. Autonegotiation is disabled. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the speed of the interface is set to 1000 Mbit/s.	Speed of the interface is 100 Mbit/s.

4.33 Duplex

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the duplexity of the interface. duplex { auto | full | half }	Mode: Interface Config Mode (Gigabitethernet interface)	1	**duplex auto**	Interface is selected. Autonegotiation is disabled. Speed is set. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the duplexity of the interface is set to auto.	Duplexity of the interface is automatic.
		2	**duplex full**	Interface is selected. Autonegotiation is disabled. Speed is set. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the duplexity of the interface is set to full.	Duplexity of the interface is full.
		3	**duplex half**	Interface is selected. Autonegotiation is disabled. Speed is set. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the duplexity of the interface is set to half.	Duplexity of the interface is half.

4.34 Autocrossing (MDI/MDIX)

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the crossing of the interface. mdix auto set port { mdi | mdix }	Mode: Interface Config Mode (Gigabitethernet interface)	1	**mdix auto**	Interface is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the crossing of the interface is set to autocrossing.	Crossing of the interface is in autocrossing mode.
		2	no mdix auto	Interface is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the auto-crossing of the interface is disabled.	Autocrossing of the interface is disabled.
		3	**set port mdi**	Interface is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the auto-crossing of the interface is set to MDI.	Crossing of the interface is set to MDI.
		4	**set port mdix**	Interface is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/x** you can check if the auto-crossing of the interface is set to MDIX.	Crossing of the interface is set to MDIX.

4.35 SNMP Trap Link-Status

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables trap generation on the interface. The no form of this command disables trap generation on the interface. The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow. snmp trap link-status no snmp trap link-status	Mode: Interface Config Mode (Gigabitethernet)	1	**snmp trap link-status**	Gi0/1 is selected. Link Up/Down Trap is Disabled. Enter the command. Using the command **show interfaces** you can check if Link Up/ Down Trap is set to Enabled.	Link Up/Down Trap is Enabled.
		2	**no snmp trap link-status**	Gi0/1 is selected. Link Up/Down Trap is Enabled. Enter the command. Using the command **show interfaces** you can check if Link Up/ Down Trap is set to Disabled.	Link Up/Down Trap is Disabled.

5. SNMPv3

5.1 SNMP User

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the SNMP user details. The no form of the command removes the SNMP user details. snmp user <UserName> [auth { md5 | sha } <passwd> [priv DES <passwd>]] [{ volatile | nonvolatile }] [EngineId <EngineID>] no snmp user <UserName> [EnginId <EngineID>]	Mode: Global Config Mode	1	**snmp user AAA auth md5 BBB priv AES_ CFB128 CCC volatile**	SNMP user AAA is not configured. Enter the command. Using the command **show snmp user** you can check if SNMP user AAA (user name, authentication protocol, privacy protocol, storage type) is configured.	SNMP user is configured. User name is AAA, authentication protocol is MD5, privacy protocol is AES_CFB128 and storage type is Volatile.
		2	**snmp user AAA auth sha BBB priv DES CCC volatile**	SNMP user AAA is configured. User name is AAA, authentication protocol is MD5, privacy protocol is AES_CFB128 and storage type is Volatile. Enter the command. Using the command **show snmp user** you can check if SNMP user details (authentication protocol, privacy protocol) are changed.	SNMP user details are changed. Authentication protocol is SHA, privacy protocol is DES.
		3	**snmp user AAA auth sha BBB priv None nonvolatile**	SNMP user AAA is configured. User name is AAA, authentication protocol is SHA, privacy protocol is DES and storage type is Volatile. Enter the command. Using the command **show snmp user** you can check if SNMP user details (privacy protocol, storage type) are changed.	SNMP user details are changed. Privacy protocol is None, storage type is Nonvolatile.

Command Description	Pre-Conditions	#	Step	Description	Result
		4	**no snmp user AAA**	SNMP user AAA is configured. User name is AAA, authentication protocol is SHA, privacy protocol is None and storage type is Nonvolatile. Enter the command. Using the command **show snmp user** you can check if SNMP user details (user name, authentication protocol, privacy protocol, storage type) are removed.	SNMP user details (user name, authentication protocol, privacy protocol, storage type) are removed.

5.2 SNMP Community Details

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the SNMP community details. The no form of this command removes the SNMP community details. snmp community index <CommunityIndex> name <CommunityName> security <SecurityName> [context <Name >] [{ volatile | nonvolatile }] [transporttag <TransportTagIdentifier | none>] [contextengineid <ContextEngineID>] no snmp community index <CommunityIndex>	Mode: Global Config Mode	1	**snmp community index ComInd name ComName security Sec context Cont contextengineid 00.11.22.33.44.55**	SNMP community with Index ComInd is not configured. Enter the command. Using the command **show snmp community** you can check if SNMP community (Community Index, Community Name, Security Name, Context Name, Context EngineId) is configured.	SNMP community is configured. Community Index is ComInd, Community Name is ComName, Security Name is Sec, Context Name is Cont, Context EngineId is 00.11.22.33.44.55.
		2	**no snmp community index ComInd**	SNMP community is configured. Community Index is ComInd, Community Name is ComName, Security Name is Sec, Context Name is Cont, Context EngineId is 00.11.22.33.44.55. Using the command **show snmp community** you can check if SNMP community with Index ComInd is removed.	SNMP community with Index ComInd is removed.

5.3 SNMP Engine ID

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination. The no form of the command resets the engine ID to the default value. - The Engine ID must be given as octets in hexadecimal separated by dots and the allowed length is 5 to 32 octets. - SNMP engine ID is an administratively unique identifier. - Changing the value of the SNMP engine ID has significant effects. - All the user information will be updated automatically to reflect the change snmp engineid <EngineIdentifier> no snmp engineid	Mode: Global Config Mode	1	**snmp engineid 00.11.22.33.44.55**	Engine ID is set to default value 80.00.08.1c.04.46.53. Enter the command. Using the command **show snmp engineid** you can check if Engine ID is set to 00.11.22.33.44.55.	Engine ID is 00.11.22.33.44.55.
		2	**no snmp engineid**	Engine ID is 00.11.22.33.44.55. Enter the command. Using the command **show snmp engineid** you can check if Engine ID is set to default value 80.00.08.1c.04.46.53.	Engine ID is 80.00.08.1c.04.46.53.

5.4 SNMP-Server Enable Traps

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables generation of a particular trap. The no form of the command disables generation of a particular trap. snmp-server enable traps { [firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsx1-line] } no snmp-server enable traps { [firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsx1-line] }	Mode: Global Config Mode	1	**snmp-server enable traps coldstart**	Generation of a trap for the Coldstart is disabled. Enter the command. Using the command **show snmp-server traps** you can check if generation of a trap for the Coldstart is enabled.	Generation of a trap for the Coldstart is enabled.
		2	**no snmp-server enable traps coldstart**	Generation of a trap for the Coldstart is enabled. Enter the command. Using the command **show snmp-server traps** you can check if generation of a trap for the Coldstart is disabled.	Generation of a trap for the Coldstart is disabled.

5.5 Show SNMP

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the status information of SNMP communications. show snmp	Mode: Privileged EXEC Mode	1	**show snmp**	Enter the command. You can check if the status information of SNMP communications is displayed.	Status information of SNMP communications is displayed.

5.6 Show SNMP Community

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the configured SNMP community details. show snmp community	Mode: Privileged EXEC Mode	1	**show snmp community**	Enter the command. You can check if configured SNMP community details are displayed.	Configured SNMP community details are displayed.

5.7 Show SNMP Engine ID

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the Engine Identifier. show snmp engineID	Mode: Privileged EXEC Mode	1	**show snmp engineID**	Enter the command. You can check if Engine Identifier is displayed.	Engine Identifier is displayed.

5.8 Show SNMP User

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the configured SNMP users. show snmp user	Mode: Privileged EXEC Mode	1	**show snmp user**	Enter the command. You can check if configured SNMP users are displayed.	Configured SNMP users are displayed.

5.9 Show SNMP Server Traps

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the set of traps that are currently enabled. show snmp-server traps	Mode: Privileged EXEC Mode	1	**show snmp-server traps**	Enter the command. You can check if the set of traps that are currently enabled is displayed.	Set of traps that are currently enabled is displayed.

6. LLDP

6.1 Shutdown LLDP

Command Description	Pre-Conditions	#	Step	Description	Result
This command shuts down all the ports in the LLDP and releases all the allocated memory. The no form of the command enables all the ports by allocating the required resources in the LLDP. shutdown lldp no shutdown lldp	Mode: Global Config Mode	1	**shutdown lldp**	LLDP is not shut down. Enter the command. Using the command **show lldp** you can check if LLDP is shut down.	LLDP is shutdown.
		2	**no shutdown lldp**	LLDP is shut down. Enter the command. Using the command **show lldp** you can check if LLDP is not shut down.	LLDP is not shutdown.

6.2 Set LLDP

Command Description	Pre-Conditions	#	Step	Description	Result
This command transmits or receives LLDP frames from the server to the LLDP module. set lldp { enable | disable }	Mode: Global Config Mode	1	**set lldp enable**	LLDP is not shut down and disabled. Enter the command. Using the command **show lldp** you can check if LLDP is enabled.	LLDP is enabled.
		2	**set lldp disable**	LLDP is not shut down and enabled. Enter the command. Using the command **show lldp** you can check if LLDP is disabled.	LLDP is disabled.

6.3 LLDP Transmit-Interval

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the transmission interval in which the server sends the LLDP frames to the LLDP module. The value ranges between 5 and 32768 seconds. The no form of the command sets the transmission interval to the default value. lldp transmit-interval <seconds(5-32768)> no lldp transmit-interval	Mode: Global Config Mode	1	**lldp transmit-interval 5**	Transmit interval is 30. Enter the command. Using the command **show lldp** you can check if Transmit interval is set to 5.	Transmit interval is 5.
		2	**lldp transmit-interval 10000**	Transmit interval is 5. Enter the command. Using the command **show lldp** you can check if Transmit interval is set to 10000.	Transmit interval is 10000.
		3	**lldp transmit-interval 32768**	Transmit interval is 10000. Enter the command. Using the command **show lldp** you can check if Transmit interval is set to 32768.	Transmit interval is 32768.
		4	**lldp transmit-interval 4**	Transmit interval is 32768. Enter the command. Using the command **show lldp** you can check if Transmit interval stays unchanged.	Transmit interval is 32768.
		5	**no lldp transmit-interval**	Transmit interval is 32768. Enter the command. Using the command **show lldp** you can check if Transmit interval is set to default value 30.	Transmit interval is 30.

6.4 LLDP Holdtime-Multiplier

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. The value ranges between 2 and 10 seconds. TLV (Time to Live) A value that tells the receiving agent, how long the information contained in the TLV Value field is valid. TTL = message transmission interval * hold time multiplier. For Example, if the value of LLDP transmission interval is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header. The no form of the command sets the multiplier to the default value lldp holdtime-multiplier <value(2-10)> no lldp holdtime-multiplier	Mode: Global Config Mode	1	**lldp holdtime-multiplier 2**	Holdtime Multiplier is 4. Enter the command. Using the command **show lldp** you can check if Holdtime Multiplier is set to 2.	Holdtime Multiplier is 2.
		2	**lldp holdtime-multiplier 6**	Holdtime Multiplier is 2. Enter the command. Using the command **show lldp** you can check if Holdtime Multiplier is set to 6.	Holdtime Multiplier is 6.
		3	**lldp holdtime-multiplier 10**	Holdtime Multiplier is 6. Enter the command. Using the command **show lldp** you can check if Holdtime Multiplier is set to 10.	Holdtime Multiplier is 10.
		4	**lldp holdtime-multiplier 1**	Holdtime Multiplier is 10. Enter the command. Using the command **show lldp** you can check if Holdtime Multiplier stays unchanged.	Holdtime Multiplier is 10.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**no lldp holdtime-multiplier**	Holdtime Multiplier is 10. Enter the command. Using the command **show lldp** you can check if Holdtime Multiplier is set to default value 4.	Holdtime Multiplier is 4.

6.5 LLDP Reinitialization-Delay

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission. The value ranges between 1 and 10 seconds. The no form of the command sets the reinitialization delay time to the default value. lldp reinitialization-delay <seconds(1-10)> no lldp reinitialization-delay	Mode: Global Config Mode	1	**lldp reinitialization-delay 1**	Reinitialization Delay is 2. Enter the command. Using the command **show lldp** you can check if Reinitialization Delay is set to 1.	Reinitialization Delay is 1.
		2	**lldp reinitialization-delay 10**	Reinitialization Delay is 5. Enter the command. Using the command **show lldp** you can check if Reinitialization Delay is set to 10.	Reinitialization Delay is 10.
		3	**no lldp reinitialization-delay**	Reinitialization Delay is 10. Enter the command. Using the command **show lldp** you can check if Reinitialization Delay is set to 2.	Reinitialization Delay is 2.

6.6 LLDP Tx-Delay

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions. The value ranges between 1 and 8192 seconds. TxDelay should be less than or equal to (0.25 * Message Tx Interval) The no form of the command sets the transmit delay to the default value. lldp tx-delay <seconds(1-8192)> no lldp tx-delay	Mode: Global Config Mode	1	**lldp tx-delay 8191**	Transmit interval is 32768. Tx Delay is 2. Enter the command. Using the command **show lldp** you can check if Tx Delay is set to 8192.	Tx Delay is 8192.
		2	**no lldp tx-delay**	Transmit interval is 32768. Tx Delay is 8192. Enter the command. Using the command **show lldp** you can check if Tx Delay is set to default value 2.	Tx Delay is 2.

6.7 LLDP Notification-Interval

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the time interval in which the local system generates a notification-event. In the specific interval, generating more than one notification-event is not possible. The value ranges between 5 and 3600 seconds. The no form of the command sets the notification interval to the default value. lldp notification-interval <seconds(5-3600)> no lldp notification-interval	Mode: Global Config Mode	1	**lldp notification-interval 5**	Notification Interval is 10. Enter the command. Using the command **show lldp** you can check if Notification Interval is set to 5.	Notification Interval is 5.
		2	**lldp notification-interval 2000**	Notification Interval is 5. Enter the command. Using the command **show lldp** you can check if Notification Interval is set to 2000.	Notification Interval is 2000.
		3	**no lldp notification-interval**	Notification Interval is 2000. Enter the command. Using the command **show lldp** you can check if Notification Interval is set to 5.	Notification Interval is 5.

6.8 LLDP Chassis-ID-Subtype

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures an ID for LLDP chassis subtype which is a unique address of any module. Chassis id value can be set only for the chassis-component and local system subtypes. For all other subtypes, it takes the value from the system automatically. lldp chassis-id-subtype { chassis-comp <string(255)> | if-alias | port-comp <string(255)> | mac-addr | nw-addr | if-name | local <string(255)> }	Mode: Global Config Mode	1	**lldp chassis-id-subtype chassis-comp aa**	Chassis ID SubType is Mac Address. Enter the command. Using the command **show lldp** you can check if Chassis ID SubType is set to Chassis Component and Chassis ID is aa.	Chassis ID SubType is Chassis Component. Chassis ID is aa.
		2	**lldp chassis-id-subtype if-alias**	Chassis ID SubType is Chassis Component. Enter the command. Using the command **show lldp** you can check if Chassis ID SubType is set to Interface Alias.	Chassis ID SubType is Interface Alias.
		3	**lldp chassis-id-subtype port-comp bb**	Chassis ID SubType is Interface Alias. Enter the command. Using the command **show lldp** you can check if Chassis Id SubType is set to Port Component and Chassis ID is bb.	Chassis ID SubType is Port Component. Chassis ID is bb.
		4	**lldp chassis-id-subtype mac-addr**	Chassis ID SubType is Port Component. Enter the command. Using the command **show lldp** you can check if Chassis ID SubType is set to Mac Address.	Chassis ID SubType is Mac Address.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**lldp chassis-id-subtype nw-addr**	Chassis ID SubType is Mac Address. Enter the command. Using the command **show lldp** you can check if Chassis ID SubType is set to Network Address.	Chassis ID SubType is Network Address.
		6	**lldp chassis-id-subtype if-name**	Chassis ID SubType is Network Address. Enter the command. Using the command **show lldp** you can check if Chassis ID SubType is set to Interface Name.	Chassis ID SubType is Interface Name.
		7	**lldp chassis-id-subtype local cc**	Chassis ID SubType is Interface Name. Enter the command. Using the command **show lldp** you can check if Chassis Id SubType is set to Local and Chassis ID is cc.	Chassis ID SubType is Port Component. Chassis ID is cc.

6.9 Clear LLDP Counters

Command Description	Pre-Conditions	#	Step	Description	Result
This command clears the inbuilt counter which has the total count of LLDP frames that are transmitted and received. This command does not clear the global statistics. clear lldp counters	Mode: Global Config Mode	1	**clear lldp counters**	LLDP is not shut down. Enter the command. Using the command **show lldp traffic** you can check if the inbuilt counter is cleared.	The inbuilt counter is cleared.

6.10 Clear LLDP Table

Command Description	Pre-Conditions	#	Step	Description	Result
This command clears all the LLDP information about the neighbors. clear lldp table	Mode: Global Config Mode	1	**clear lldp table**	LLDP is not shut down. Enter the command. Using the command **show lldp neighbors** you can check if all LLDP information about the neighbors is cleared.	All LLDP information about the neighbors is cleared.

6.11 LLDP

Command Description	Pre-Conditions	#	Step	Description	Result
This command transmits or receives LLDP frames from the one of the ports of the server to the LLDP module. The no form of the command resets LLDP admin status on an interface. lldp { transmit | receive } no lldp { transmit | receive }	Mode: Interface Config Mode	1	**lldp transmit**	Gi0/8 is selected. LLDP is not shut down. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if transmission of LLDPDU from one of the ports of the server to the LLDP module is enabled.	Transmission of LLDPDU from one of the ports of the server to the LLDP module is enabled.
		2	**lldp receive**	Gi0/8 is selected. LLDP is not shut down. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if reception of LLDPDU from one of the ports of the server to the LLDP module is enabled.	Reception of LLDPDU from one of the ports of the server to the LLDP module is enabled.
		3	**no lldp transmit**	Gi0/8 is selected. LLDP is not shut down. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if transmission of LLDPDU from one of the ports of the server to the LLDP module is disabled.	Transmission of LLDPDU from one of the ports of the server to the LLDP module is disabled.
		4	**no lldp receive**	Gi0/8 is selected. LLDP is not shut down. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if reception of LLDPDU from one of the ports of the server to the LLDP module is disabled.	Reception of LLDPDU from one of the ports of the server to the LLDP module is disabled.

6.12 LLDP Notification

Command Description	Pre-Conditions	#	Step	Description	Result
This command controls the transmission of LLDP notifications. The no form of the command disables LLDP trap notification on an interface. lldp notification [remote-table-chg] [mis-configuration] no lldp notification	Mode: Interface Config Mode	1	**lldp notification**	Gi0/8 is selected. LLDP is not shut down. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if the transmission of LLDP notifications is enabled and Notification Type is set to Mis-Configuration.	Transmission of LLDP notifications is enabled. Notification Type is Mis-Configuration.
		2	**lldp notification remote-table-chg**	Gi0/8 is selected. LLDP is not shut down. Notification Type is Mis-Configuration. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if the transmission of LLDP notifications is enabled and Notification Type is set to Remote Table Change.	Transmission of LLDP notifications is enabled. Notification Type is Remote Table Change.
		3	**lldp notification mis-configuration**	Gi0/8 is selected. LLDP is not shut down. Notification Type is Remote Table Change. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if the transmission of LLDP notifications is enabled and Notification Type is set to Mis-Configuration.	Transmission of LLDP notifications is enabled. Notification Type is Mis-Configuration.

Command Description	Pre-Conditions	#	Step	Description	Result
		4	**no lldp notification**	Gi0/8 is selected. LLDP is not shut down. Notification Type is Remote Table Change. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if the transmission of LLDP notifications is disabled and Notification Type is set to default value Mis-Configuration.	Transmission of LLDP notifications is disabled. Notification Type is Mis-Configuration.

6.13 LLDP TLV-Select Basic-TLV

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the basic settings while transmitting the LLDP frames on a given port. The no form of the command disables the basic TLV transmission on a given port. lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr { all | ipv4 <ucast_addr> }] } no lldp tlv-select basic-tlv { [port-descr] [sys-name] [sys-descr] [sys-capab] [mgmt-addr { all | ipv4 <ucast_addr> }] }	Mode: Interface Config Mode	1	**lldp tlv-select basic-tlv port-descr sys-name sys-descr sys-capab mgmt-addr all**	Gi0/8 is selected. LLDP is not shut down. Enabled Tx TLVs: None. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if Enabled Tx TLVs are Port Description, System Name, System Description, System Capability, Management Address.	Enabled Tx TLVs: Port Description, System Name, System Description, System Capability, Management Address.
		2	**no lldp tlv-select basic-tlv port-descr sys-name sys-descr sys-capab**	Gi0/8 is selected. LLDP is not shut down. Enabled Tx TLVs: Port Description, System Name, System Description, System Capability, Management Address. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if Enabled Tx TLVs are Management Address.	Enabled Tx TVLs: Management Address.

6.14 LLDP Port-ID-Subtype

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures an ID for LLDP port subtype lldp port-id-subtype { if-alias | port-comp <string(255)> | mac-addr | if-name | local <string(255)> }	Mode: Interface Config Mode	1	**lldp port-id-subtype if-alias**	Gi0/8 is selected. LLDP is not shut down. Port Id SubType: Mac Address. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if Port Id SubType is set to Interface Alias.	Port Id SubType: Interface Alias
		2	**lldp port-id-subtype port-comp pp**	Gi0/8 is selected. LLDP is not shut down. Port Id SubType: Interface Alias. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if Port Id SubType is set to Port Component and Port Id is pp.	Port Id SubType: Port Component Port Id: pp
		3	**lldp port-id-subtype mac-addr**	Gi0/8 is selected. LLDP is not shut down. Port Id SubType: Port Component. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if Port Id SubType is set to Mac Address.	Port Id SubType: Mac Address
		4	**lldp port-id-subtype if-name**	Gi0/8 is selected. LLDP is not shut down. Port Id SubType: Mac Address. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if Port Id SubType is set to Interface Name.	Port Id SubType: Interface Name

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**lldp port-id-subtype local bb**	Gi0/8 is selected. LLDP is not shut down. Port Id SubType: Interface Name. Enter the command. Using the command **show lldp interface gigabitethernet 0/8** you can check if Port Id SubType is set to Local and Port Id is bb.	Port Id SubType: Local Port Id: bb

6.15 LLDP TLV-Select Dot1TLV

Command Description	Pre-Conditions	#	Step	Description	Result
Performs dot1 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings. The no form of the command disables the transmission of dot1 TLV types on a port. lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}] no lldp tlv-select dot1tlv {[port-vlan-id] [protocol-vlan-id {all |<vlan-id>}] [vlan-name {all | <vlan-id>}]}	Mode: Interface Config Mode	1	**lldp tlv-select dot1tlv port-vlan-id** **protocol-vlan-id 42**	Configure TLV settings for VLAN 42.	**show lldp local** should show the configured values.

6.16 LLDP TLV-Select Dot3TLV

Command Description	Pre-Conditions	#	Step	Description	Result
This command performs dot3 TLV configuration while transmitting the LLDP frames to the particular port apart from the basic settings. The no form of the command disables the transmission of dot3 TLV types on a port. lldp tlv-select dot3tlv { [macphy-config] [link-aggregation] [max-framesize] } no lldp tlv-select dot3tlv { [macphy-config] [link-aggregation] [maxframesize] }	Mode: Interface Config Mode	1	**lldp tlv-select dot3tlv macphy-config link-aggregation max-framesize**	Gi0/8 is selected. LLDP is not shut down. Enabled Tx TLVs: None. Enter the command. Using the command **show lldp local gigabitethernet 0/8** you can check if Enabled Tx TLVs are Mac Phy, Link Aggregation and Max Frame Size.	Enabled Tx TLVs: Mac Phy, Link Aggregation, Max Frame Size.
		2	**no lldp tlv-select dot3tlv macphy-config link-aggregation**	Gi0/8 is selected. LLDP is not shut down. Enabled Tx TLVs: Mac Phy, Link Aggregation, Max Frame Size. Enter the command. Using the command **show lldp local gigabitethernet 0/8** you can check if Enabled Tx TLVs are Max Frame Size.	Enabled Tx TLVs: Max Frame Size.

6.17 LLDP Dest-MAC

Command Description	Pre-Conditions	#	Step	Description	Result
Configures destination mac-address to be used by the LLDP agent for transmission. The no form of the command disables the feature. lldp dest-mac <mac_addr> no lldp dest-mac <mac_addr>	Mode: Port Config Mode	1	**lldp dest-mac 00:01:02:03:04:05**	Set the destination mac-address to 00:01:02:03:04:05.	**show lldp interface gigabitethernet X/X** should show the configured mac-address for port X/X.

6.18 Show LLDP

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays LLDP global configuration details to initialize on an interface. show lldp	Mode: Privileged EXEC Mode	1	**show lldp**	LLDP is not shut down. Enter the command. You can check if LLDP global configuration details are displayed.	LLDP global configuration details are displayed.

6.19 Show LLDP Interface

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the information about interfaces where LLDP is enabled. show lldp interface [<interface-type> <interface-id>]		1	show lldp interface	Enter the command. You can check if information about interfaces where LLDP is enabled is displayed.	Information about interfaces is displayed.
		2	**show lldp interface gigabitethernet 0/8**	Enter the command. You can check if information about the specified type of interface (Gi0/8) is displayed.	Information about the specified type of interface (Gi0/8) is displayed.

6.20 Show LLDP Neighbors

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays information about neighbors on an interface or all interfaces. show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interface-type> <interface-id>] [detail]	Mode: Privileged EXEC Mode	1	**show lldp neighbors**	Enter the command. You can check if information about neighbors on all interfaces is displayed.	Information about neighbors on all interfaces is displayed.
		2	**show lldp neighbors detail**	Enter the command. You can check if information obtained from all the received TLVs about neighbors on all interfaces is displayed.	Information obtained from all the received TLVs about neighbors on all interfaces is displayed.
		3	**show lldp neighbors gigabitethernet 0/8**	Enter the command. You can check if information about neighbors on the specified interface (Gi0/8) is displayed.	Information about neighbors on the specified interface (Gi0/8) is displayed.
		4	**show lldp neighbors gigabitethernet 0/8 detail**	Enter the command. You can check if information obtained from all the received TLVs about neighbors on the specified interface (Gi0/8) is displayed.	Information obtained from all the received TLVs about neighbors on the specified interface (Gi0/8) is displayed.

6.21 Show LLDP Traffic

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays LLDP counters on all interfaces or on a specific interface. This includes the following: - Total Frames Out - Total Entries Aged - Total Frames In - Total Frames Received In Error - Total Frames Discarded - Total TLVS Unrecognized - Total TLVs Discarded show lldp traffic [<iftype> <ifnum>]	Mode: Privileged EXEC Mode	1	**show lldp traffic**	Enter the command. You can check if LLDP counters (Total Frames Out, Total Entries Aged, Total Frames In, Total Frames Received In Error, Total Frames Discarded, Total TLVS Unrecognized, Total TLVs Discarded) on all interfaces are displayed.	LLDP counters (Total Frames Out, Total Entries Aged, Total Frames In, Total Frames Received In Error, Total Frames Discarded, Total TLVS Unrecognized, Total TLVs Discarded) on all interfaces are displayed.
		2	**show lldp traffic gigabitethernet 0/8**	Enter the command. You can check if LLDP counters (Total Frames Out, Total Entries Aged, Total Frames In, Total Frames Received In Error, Total Frames Discarded, Total TLVS Unrecognized, Total TLVs Discarded) on the specified interface (Gi0/8) are displayed.	LLDP counters (Total Frames Out, Total Entries Aged, Total Frames In, Total Frames Received In Error, Total Frames Discarded, Total TLVS Unrecognized, Total TLVs Discarded) on the specified interface (Gi0/8) are displayed.

6.22 Show LLDP Local

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces. show lldp local { [<interface-type> <interface-id>] | [mgmt-addr] }	Mode: Privileged EXEC Mode	1	**show lldp local**	Enter the command. You can check if the current switch information that will be used to populate outbound LLDP advertisements for all interfaces is displayed.	Current switch information that will be used to populate outbound LLDP advertisements for all interfaces is displayed.
		2	**show lldp local gigabitethernet 0/8**	Enter the command. You can check if the current switch information that will be used to populate outbound LLDP advertisements for the specified interface (Gi0/8) is displayed.	Current switch information that will be used to populate outbound LLDP advertisements for the specified interface (Gi0/8) is displayed.

6.23 Show LLDP Errors

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the information about the errors such as memory allocation failures, queue overflows and table overflow. show lldp errors	Mode: Privileged EXEC Mode	1	**show lldp errors**	Enter the command. You can check if the information about the errors such as memory allocation failures, queue overflows and table overflow is displayed.	The information about the errors such as memory allocation failures, queue overflows and table overflow is displayed.

6.24 Show LLDP Statistics

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the LLDP remote table statistics information. show lldp statistics	Mode: Privileged EXEC Mode	1	**show lldp statistics**	Enter the command. You can check if the LLDP remote table statistics information is displayed.	The LLDP remote table statistics information is displayed.

7. DHCP

7.1 Release DHCP

Command Description	Pre-Conditions	#	Step	Description	Result
This command immediately releases the DHCP lease obtained for an IP address from a DHCP server and assigned to the specified interface. The current lease assigned to that interface is terminated manually. The lease is terminated to reset the DHCP client which faces connectivity problem. The DHCP lease provided by the DHCP server represents the time interval till which the DHCP client can use the assigned IP address. release dhcp { vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }	Mode: Privileged EXEC Mode	1	**release dhcp vlan 1**	Enter the command. Using the command **show ip dhcp client stats** you can check if DHCP lease is released for the specified interface.	DHCP lease is released.
		2	**release dhcp gigabitethernet 0/1**	Enter the command. Using the command **show ip dhcp client stats** you can check if DHCP lease is released for the specified interface.	DHCP lease is released.

7.2 Renew DHCP

Command Description	Pre-Conditions	#	Step	Description	Result
This command immediately renews the DHCP lease for the interface specified. The current lease acquired by the specified interface is manually renewed or else a new DHCP lease is acquired for interface whose lease is terminated. The DHCP lease is automatically renewed, once the lease expires. renew dhcp { vlan <vlan-id (1-4094)> | <interface-type> <interface-id> }	Mode: Privileged EXEC Mode	1	**renew dhcp vlan 2**	Enter the command. Using the command **show ip dhcp client stats** you can check if DHCP lease is renewed for the specified interface.	DHCP lease is renewed.
		2	**renew dhcp gigabitethernet 0/1**	Enter the command. Using the command **show ip dhcp client stats** you can check if DHCP lease is renewed for the specified interface.	DHCP lease is renewed.

7.3 Show IP DHCP Client Stats

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server. The statistics information contains interface name, IP address assigned by DHCP server, DHCP lease details, details regarding number of DHCPDISCOVER, DHCPREQUEST, DHCPDECLINE, DHCPRELEASE and DHCPINFORM packets received and number of DHCPOFFER packets sent from the DHCP client. show ip dhcp client stats	Mode: Privileged EXEC Mode	1	**show ip dhcp client stats**	Enter the command. You can check if DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server is displayed.	DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server is displayed.

7.4 Service DHCP-Relay

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the DHCP relay agent in the switch. The no form of the command disables the DHCP relay agent. DHCP relay agent relays DHCP messages between DHCP client and DHCP server located in different subnets. service dhcp-relay no service dhcp-relay	Mode: Global Config Mode	1	**service dhcp-relay**	DHCP Relay is disabled. Enter the command. Using the command **show ip dhcp relay information** you can check if DHCP Relay is enabled.	DHCP Relay is enabled.
		2	**no service dhcp-relay**	DHCP Relay is enabled. Enter the command. Using the command **show ip dhcp relay information** you can check if DHCP Relay is disabled.	DHCP Relay is disabled.

7.5 IP DHCP Server

Command Description	Pre-Conditions	#	Step	Description	Result
This command adds the configured IP address to the IP address list created for the DHCP server. The switches or systems having these IP addresses represent the DHCP servers to which the DHCP relay agent can forward the packets that are received from DHCP clients. The no form of the command deletes the mentioned IP address from the IP address list. The DHCP relay agent broadcasts the received packets to entire network except the network from which the packets are received, if the DHCP server list is empty (that is IP address is configured as 0.0.0.0). Note: The IP address list can contain only 5 IP addresses (that is, only a maximum of 5 DHCP servers can be listed). ip dhcp server <ip address> no ip dhcp server <ip address>	Mode: Global Config Mode	1	**ip dhcp server 192.168.0.51**	DHCP Server List doesn't contain 192.168.0.51. Enter the command. Using the command **show ip dhcp relay information** you can check if DHCP Server List contains 192.168.0.51.	192.168.0.51 is in the DHCP Server List.
		2	no ip dhcp server 192.168.0.51	DHCP Server List contains 192.168.0.51. Enter the command. Using the command **show ip dhcp relay information** you can check if DHCP Server List doesn't contain 192.168.0.51.	192.168.0.51 is not in the DHCP Server List.

7.6 IP DHCP Relay Information Option

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the DHCP relay agent to perform processing related to DHCP relay agent information option. The no form of the command disables the processing related to DHCP relay agent information option. The options contains a sub-option for agent circuit ID details and another sub-option for agent remote ID details. The processing involves: - Insertion of DHCP relay information option in DHCP request messages forwarded to a DHCP server from a DHCP client. - Examining / removing of DHCP relay information option from DHCP response messages forwarded to the DHCP client from the DHCP server. ip dhcp relay information option no ip dhcp relay information option	Mode: Global Config Mode	1	**ip dhcp relay information option**	DHCP Relay RAI option is disabled. Enter the command. Using the command **show ip dhcp relay information** you can check if DHCP Relay RAI option is enabled.	DHCP Relay RAI option is enabled.
		2	**no ip dhcp relay information option**	DHCP Relay RAI option is enabled. Enter the command. Using the command **show ip dhcp relay information** you can check if DHCP Relay RAI option is disabled.	DHCP Relay RAI option is disabled.

7.7 IP DHCP Relay Circuit-ID Option

Command Description	Pre-Conditions	#	Step	Description	Result
This command defines the type of information to be present in Circuit ID suboption that is used in the DHCP relay agent information option. ip dhcp relay circuit-id option [router-index] [vlanid] [recv-port]	Mode: Global Config Mode	1	**ip dhcp relay circuit-id option router-index**	DHCP Relay RAI option is enabled. Default Circuit ID Information is VLAN ID. Enter the command. Using the command **show ip dhcp relay information** you can check if Default Circuit ID Information is set to Router-index.	Default Circuit ID Information is Router-index.
		2	**ip dhcp relay circuit-id option router-index vlanid**	DHCP Relay RAI option is enabled. Default Circuit ID Information is Recv-Port. Enter the command. Using the command **show ip dhcp relay information** you can check if Default Circuit ID Information is set to Router-index and VLAN ID.	Default Circuit ID Information is Router-index and VLAN ID.
		3	**ip dhcp relay circuit-id option router-index recv-port**	DHCP Relay RAI option is enabled. Default Circuit Id Information is VlanId. Enter the command. Using the command **show ip dhcp relay information** you can check if Default Circuit ID Information is set to Router-index and Recv-Port.	Default Circuit ID Information is Router-index and Recv-Port.
		4	**ip dhcp relay circuit-id option router-index vlanid recv-port**	DHCP Relay RAI option is enabled. Default Circuit ID Information is VLAN ID. Enter the command. Using the command **show ip dhcp relay information** you can check if Default Circuit ID Information is set to Router-index, VLAN ID and Recv-Port.	Default Circuit ID Information is Router-index, VlanId and Recv-Port.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**ip dhcp relay circuit-id option vlanid**	DHCP Relay RAI option is enabled. Default Circuit ID Information is Router-index. Enter the command. Using the command **show ip dhcp relay information** you can check if Default Circuit ID Information is set to VLAN ID.	Default Circuit ID Information is VLAN ID.
		6	ip dhcp relay circuit-id option vlanid recv-port	DHCP Relay RAI option is enabled. Default Circuit ID Information is Router-index. Enter the command. Using the command **show ip dhcp relay information** you can check if Default Circuit ID Information is set to VLAN ID and Recv-Port.	Default Circuit ID Information is VLAN ID and Recv-Port.
		7	**ip dhcp relay circuit-id option recv-port**	DHCP Relay RAI option is enabled. Default Circuit ID Information is Router-index. Enter the command. Using the command **show ip dhcp relay information** you can check if Default Circuit ID Information is set to Recv-Port.	Default Circuit ID Information is Recv-Port.

7.8 IP DHCP Relay Circuit-ID

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures circuit ID value for an interface. The no form of the command deletes the Circuit ID configuration for the interface (that is, the Circuit ID is configured as 0). The Circuit ID uniquely identifies a Circuit over which the incoming DHCP packet is received. In DHCP relay, it is used to identify the correct circuit over which the DHCP responses should be relayed. The configured Circuit ID is used in the DHCP relay agent information option to inform the DHCP server about the interface from which DHCP packet is received. The Circuit ID is unique for the interfaces and ranges from 1 to 2147483647. The minimum value depends upon the number of interfaces that can be created. For example, if a total of 160 interfaces are allowed to be created in the switch, then the Circuit ID value range starts from 161 only. The interfaces include all physical interfaces, port channels and logical L3 interfaces. ip dhcp relay circuit-id <circuit-id> no ip dhcp relay circuit-id	Mode: Interface Config Mode	1	ip dhcp relay circuit-id 1	Circuit ID value for an interface is not configured. Enter the command. Using the command **show ip dhcp relay information** you can check if Circuit ID for the specified VLAN is set to 1.	Circuit ID for the specified VLAN is 1.
		2	no ip dhcp relay circuit-id	Enter the command. Using the command **show ip dhcp client stats** you can check if DHCP lease is released for the specified interface.	Circuit ID for the specified VLAN is removed

7.9 IP DHCP Relay Remote-ID

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures Remote ID value for an interface. The no form of the command deletes the Remote ID configuration for the interface (that is, the Remote ID is set with a string of length zero). The configured Remote ID is used to inform the DHCP client about the remote circuit to which the DHCP packets should be forwarded from the interface. The Remote ID is globally unique and an octet string of maximum size of 32. The Remote ID should not be same as that of the default value. ip dhcp relay remote-id <remote-id name> no ip dhcp relay remote-id	Mode: Interface Config Mode	1	**ip dhcp relay remote-id DDD1**	Remote ID value for an interface is not configured. Enter the command. Using the command **show ip dhcp relay information** you can check if Remote ID for the specified VLAN is set to DDD1.	Remote ID for the specified VLAN is DDD1.
		2	**no ip dhcp relay remote-id**	Remote ID value for an interface is configured. Enter the command. Using the command **show ip dhcp relay information** you can check if Remote ID for the specified VLAN is removed.	Remote ID for the specified VLAN is removed.

7.10 Show IP DHCP Relay Information

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured. The information contains status of the DHCP relay, DHCP server IP addresses, status of relay information option, configured debug level and statistics details regarding number of packets affected by relay information option, Circuit ID suboption, Remote ID suboption, and subnet mask sub option. show ip dhcp relay information [vlan <vlan-id>]	Mode: Privileged EXEC Mode	1	**show ip dhcp relay information**	Enter the command. You can check if DHCP relay agent configuration information (status of the DHCP relay, DHCP server IP addresses, status of relay information option, configured debug level and statistics details regarding number of packets affected by relay information option, circuit ID suboption, remote ID suboption, and subnet mask sub option) for a specific VLAN interface or all interfaces in which relay agent details are configured is displayed.	DHCP relay agent configuration information for a specific VLAN interface or all interfaces in which relay agent details are configured is displayed.
		2	show ip dhcp relay information vlan 1	DHCP relay agent for the specified VLAN ID is configured. Enter the command. You can check if DHCP relay agent configuration information for the specified VLAN ID is displayed.	DHCP relay agent configuration information for the specified VLAN ID is displayed.

7.11 Show DHCP Server

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the DHCP servers' IP addresses. These addresses denotes the PCs or switches that can act as a DHCP server. show dhcp server	Mode: Privileged EXEC Mode	1	**show dhcp server**	DHCP Server List contains IP addresses e.g. 192.168.0.51, 192.168.0.52, 192.168.0.53. Enter the command. You can check if the DHCP servers' IP addresses are displayed.	DHCP servers' IP addresses are displayed.

8. (Rapid) Spanning Tree Protocol (RSTP, STP)

8.1 Shutdown Spanning-Tree

Command Description	Pre-Conditions	#	Step	Description	Result
This command shuts down spanning tree functionality in the switch. The switch does not execute any kind of STP to form a loop free topology in the Ethernet network and operates with the existing topology structure. shutdown spanning-tree	Mode: Global Config Mode	1	**shutdown spanning-tree**	Spanning tree is enabled. Enter the command. You can check if spanning tree is shut down.	Spanning Tree is shutdown.

8.2 Spanning-Tree

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the spanning tree operation in the switch for the selected spanning tree mode. Spanning tree operation provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. It logically breaks such loops and prevents looping traffic from clogging the network. The no form of this command disables the spanning tree operation in the switch. The spanning tree operation is automatically enabled in the switch, once the spanning tree mode is changed. spanning-tree no spanning-tree	Mode: Global Config Mode	1	**spanning-tree**	Spanning tree functionality is not shut down. Spanning Tree Operation is disabled. Enter the command. Using the command **show spanning-tree active** you can check if Spanning Tree Operation (Protocol) is enabled.	Spanning Tree Protocol is enabled.
		2	**no spanning-tree**	Spanning tree functionality is not shut down. Spanning Tree Operation is enabled. Enter the command. Using the command **show spanning-tree active** you can check if Spanning Tree Operation (Protocol) is disabled.	Spanning Tree Protocol is disabled.

8.3 Spanning-Tree ForwardTime/HelloTime/MaxAge

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology. The no form of this command resets the spanning tree timers to its default values. The spanning tree timers are reset to its default value, even if the spanning tree mode is changed. spanning-tree { forward-time <seconds(4-30)> | hello-time <seconds(1-2)> | maxage <seconds(6-40)> } no spanning-tree { forward-time | hello-time | max-age }	Mode: Global Config Mode	1	**spanning-tree forward-time 10**	Forward Time = 15 Hello Time = 2 Max Age = 20 Conditions to satisfy: 1) 2 * (Forward-Time - 1) >= Max-Age 2) Max-Age >= 2 * (Hello-Time +1) Enter the command. Using the command **show spanning-tree detail** you can check if Forward Time stays at 15.	Forward Time is 15, because the conditions are not satisfied.
		2	spanning-tree forward-time 11	Forward Time = 15 Hello Time = 2 Max Age = 20 Conditions to satisfy: 1) 2 * (Forward-Time - 1) >= Max-Age 2) Max-Age >= 2 * (Hello-Time +1) Enter the command. Using the command **show spanning-tree detail** you can check if Forward Time is set to 11.	Forward Time is 11.
		3	**spanning-tree hello-time 1**	Forward Time = 15 Hello Time = 2 Max Age = 20 Conditions to satisfy: 1) 2 * (Forward-Time - 1) >= Max-Age 2) Max-Age >= 2 * (Hello-Time +1) Enter the command. Using the command **show spanning-tree detail** you can check if Hello Time is set to 1.	Hello Time is 1.

Command Description	Pre-Conditions	#	Step	Description	Result
		4	**spanning-tree max-age 30**	Forward Time = 15 Hello Time = 2 Max Age = 20 Conditions to satisfy: 1) 2 * (Forward-Time - 1) >= Max-Age 2) Max-Age >= 2 * (Hello-Time +1) Enter the command. Using the command **show spanning-tree detail** you can check if Max Age stays at 20.	Max Age is 20, because the conditions are not satisfied.
		5	**spanning-tree max-age 28**	Forward Time = 15 Hello Time = 2 Max Age = 20 Conditions to satisfy: 1) 2 * (Forward-Time - 1) >= Max-Age 2) Max-Age >= 2 * (Hello-Time +1) Enter the command. Using the command **show spanning-tree detail** you can check if Max Age is set to 28.	Max Age is 28.

8.4 Spanning-Tree Transmit Hold-Count

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the transmit hold-count value for the switch. The no form of this command sets the transmit hold-count to its default value. The transmit hold-count is changed to its default value even if the spanning tree mode is changed. The transmit hold count value is a counter that is used to limit the maximum transmission rate of the switch and to avoid flooding. This value specifies the maximum number of packets that can be sent in a given hello time interval. This value ranges between 1 and 10. spanning-tree transmit hold-count <value (1-10)> no spanning-tree transmit hold-count	Mode: Global Config Mode	1	**spanning-tree transmit hold-count 10**	Transmit Hold-Count is 1. Enter the command. Using the command **show spanning-tree detail** you can check if Transmit Hold-Count is set to 10.	Transmit Hold-Count is 10.
		2	**no spanning-tree transmit hold-count**	Transmit Hold-Count is 10. Enter the command. Using the command **show spanning-tree detail** you can check if Transmit Hold-Count is set to 6.	Transmit Hold-Count is 6.

8.5 Clear Spanning-Tree Counters

Command Description	Pre-Conditions	#	Step	Description	Result
This command deletes all bridge and port level spanning tree statistics information. clear spanning-tree [mst <instance-id>] counters [interface <interface-type> <interface-id>]	Mode: Global Config Mode. Spanning tree functionality is not shutdown.	1	**clear spanning-tree counters**	Enter the command. Using the command **show spanning-tree detail** you can check if all bridge and port level spanning tree statistics information for all ports is deleted.	All bridge and port level spanning tree statistics information for all ports is deleted.
		2	**clear spanning-tree counters interface gigabitethernet 0/8**	Enter the command. Using the command **show spanning-tree detail** you can check if all port-level spanning-tree statistics information for the port gigabitethernet 0/8 is deleted.	All port-level spanning-tree statistics information for the port gigabitethernet 0/8 is deleted.

8.6 Spanning-Tree Pathcost Dynamic

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables dynamic pathcost calculation feature in the switch. The no form of this command disables dynamic pathcost calculation feature in the switch. The dynamic pathcost calculation feature is disabled, even if the spanning tree mode is changed. The path cost of the port / MSTI is dynamically calculated. This feature is applied only for the ports that are not shutdown during the execution of STP. The calculated path cost is not changed based on the operational status of the port / for a MSTI, once calculated. The manually assigned / already calculated path cost is used even if the dynamic pathcost calculation feature is enabled in the switch. spanning-tree pathcost dynamic [lag-speed] no spanning-tree pathcost dynamic [lag-speed]	Mode: Global Config Mode, Spanning tree functionality is not shutdown	1	**spanning-tree pathcost dynamic**	Dynamic Path Cost is disabled. Enter the command. Using the command **show spanning-tree active** you can check if Dynamic Path Cost is enabled.	Dynamic Path Cost is enabled.
		2	**spanning-tree pathcost dynamic lag-speed**	Dynamic Path Cost is disabled. Dynamic Path Cost Lag-Speed Change is disabled. Enter the command. Using the command **show spanning-tree active** you can check if Dynamic Path Cost Lag-Speed Change is disabled, because dynamic pathcost calculation feature is disabled.	Dynamic Path Cost Lag-Speed Change is disabled.

Command Description	Pre-Conditions	#	Step	Description	Result
		3	**spanning-tree pathcost dynamic lag-speed**	Dynamic Path Cost is enabled. Dynamic Path Cost Lag-Speed Change is disabled. Enter the command. Using the command **show spanning-tree active** you can check if Dynamic Path Cost Lag-Speed Change is enabled.	Dynamic Path Cost Lag-Speed Change is enabled.
		4	**no spanning-tree pathcost dynamic lag-speed**	Dynamic Path Cost is enabled. Dynamic Path Cost Lag-Speed Change is enabled. Enter the command. Using the command **show spanning-tree active** you can check if Dynamic Path Cost Lag-Speed Change is disabled.	Dynamic Path Cost Lag-Speed Change is disabled.
		5	**no spanning-tree pathcost dynamic**	Dynamic Path Cost is enabled. Enter the command. Using the command **show spanning-tree active** you can check if Dynamic Path Cost is disabled.	Dynamic Path Cost is disabled.

8.7 Spanning-Tree Priority

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the priority value that is assigned to the switch. The no form of this command resets the priority to its default value. The priority value is changed to its default value even if the spanning tree mode is changed. In RSTP, this value is used during the election of root. spanning-tree priority <value(0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)> no spanning-tree priority	Mode: Global Config Mode	1	**spanning-tree priority 0**	Priority is 32768. Enter the command. Using the command **show spanning-tree** you can check if Priority (Bridge ID) is set to 0.	Priority is 0.
		2	**spanning-tree priority 8192**	Priority is 32768. Enter the command. Using the command **show spanning-tree** you can check if Priority (Bridge ID) is set to 8192.	Priority is 8192.
		3	**no spanning-tree priority**	Priority is 0. Enter the command. Using the command **show spanning-tree** you can check if Priority (Bridge ID) is set to 32768.	Priority is 32768.

8.8 Spanning-Tree Auto-Edge

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables automatic detection of Edge port parameter of an interface. The no form of this command disables automatic detection of Edge port parameter of an interface. The automatic detection of Edge port parameter is disabled, even if the spanning tree mode is changed. Once automatic detection is enabled, the Edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non -edge port, if any BPDU is received. spanning-tree auto-edge no spanning-tree auto-edge	Mode: Interface Config Mode (Physical Interface Mode)	1	**spanning-tree auto-edge**	Auto-Edge is disabled. Enter the command. Using the command **show spanning-tree detail** you can check if Auto-Edge is enabled.	Auto-Edge is enabled.
		2	**no spanning-tree auto-edge**	Auto-Edge is enabled. Enter the command. Using the command **show spanning-tree detail** you can check if Auto-Edge is disabled.	Auto-Edge is disabled.

8.9 Spanning-Tree Interface

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the port related spanning tree information for all kinds of STPs. This can be applied for any port, in RSTP mode. The no form of this command resets the port related spanning tree information to its default value. The port related spanning tree information is changed to its default value even if the spanning tree mode is changed. spanning-tree { cost <value(0-200000000)> | disable | link-type { point-to-point | shared } | portfast | port-priority <value(0-240)> } no spanning-tree { cost | disable | link-type | portfast | port-priority }	Mode. Interface Config Mode (Physical Interface Mode)	1	**spanning-tree cost 2000**	Physical Interface: Gigabitethernet 0/3 Path Cost is 2000000. Enter the command. Using the command **spanning-tree interface gigabitethernet 0/3 detail** you can check if Path Cost is set to 2000.	Path Cost is 2000.
		2	**spanning-tree link-type point-to-point**	Link Type is Shared. Enter the command. Using the command **spanning-tree interface gigabitethernet 0/3 detail** you can check if Link Type is set to Point-to-Point.	Link Type is Point-to-Point.
		3	**spanning-tree link-type shared**	Link Type is Point to Point. Enter the command. Using the command **spanning-tree interface gigabitethernet 0/3 detail** you can check if Link Type is set to Shared.	Link Type is Shared.
		4	**spanning-tree port-priority 16**	Port Priority is 0. Enter the command. Using the command **spanning-tree interface gigabitethernet 0/3 detail** you can check if Port Priority is set to 16.	Port Priority is 16.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**spanning-tree disable**	Gigabitethernet Port (0/3) RSTP Status is enabled. Enter the command. Using the command **spanning-tree interface gigabitethernet 0/3 detail** you can check if Port RSTP Status is set to disabled.	Port RSTP Status is disabled.
		6	**no spanning-tree disable**	Gigabitethernet Port (0/3) RSTP Status is disabled. Enter the command. Using the command **spanning-tree interface gigabitethernet 0/3 detail** you can check if Port RSTP Status is set to enabled.	Port RSTP Status is enabled.
		7	spanning-tree portfast	Gigabitethernet Port (0/3) PortFast is disabled. Enter the command. Using the command **spanning-tree interface gigabitethernet 0/3 detail** you can check if PortFast is set to enabled.	PortFast is enabled.
		8	**no spanning-tree portfast**	Gigabitethernet Port (0/3) PortFast is enabled. Enter the command. Using the command **spanning-tree interface gigabitethernet 0/3 detail** you can check if PortFast is set to disabled.	PortFast is disabled.

8.10 Spanning-Tree Restricted-Role

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the restricted role feature for a port. The restricted role feature blocks the port from being selected as a root port even if it has the best spanning tree priority vector. This port is selected as an alternate port after the root port is selected. This feature allows you to block switches external to a core region of the network from influencing the spanning tree active topology. The blocking of port from being selected as a root port can cause lack of spanning tree connectivity. The no form of this command disables the restricted role feature in the port. The restricted role feature is disabled, even if the spanning tree mode is changed. spanning-tree restricted-role no spanning-tree restricted-role	Mode: Interface Config Mode (Physical Interface Mode)	1	**spanning-tree restricted-role**	Restricted Role is disabled. Enter the command. Using the command **show spanning-tree detail** you can check if Restricted Role is enabled.	Restricted Role is enabled.
		2	**no spanning-tree restricted-role**	Restricted Role is enabled. Enter the command. Using the command **show spanning-tree detail** you can check if Restricted Role is disabled.	Restricted Role is disabled.

8.11 Spanning-Tree Restricted-TCN

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the topology change guard / restricted TCN feature on a port. The restricted TCN feature blocks the port from propagating the received topology change notifications and topology changes to other ports. This feature allows you to block switches external to a core region of the network from causing address flushing in the region. The blocking of port can cause temporary loss of connectivity after changes in a spanning tree active topology as a result of persistent incorrectly learnt station location information. The no form of this command disables the topology change guard / restricted TCN feature on the port. The topology change guard / restricted TCN feature is disabled, even if the spanning tree mode is changed. spanning-tree restricted-tcn no spanning-tree restricted-tcn	Mode: Interface Config Mode (Physical Interface Mode)	1	**spanning-tree restricted-tcn**	Restricted TCN is disabled. Enter the command. Using the command **show spanning-tree detail** you can check if Restricted TCN is enabled.	Restricted TCN is enabled.
		2	**no spanning-tree restricted-tcn**	Restricted TCN is enabled. Using the command **show spanning-tree detail** you can check if Restricted TCN is disabled.	Restricted TCN is disabled.

8.12 Spanning-Tree BDPU-Receive

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the processing status of the BPDUs received in a port. BPDUs are used to carry bridge related information that is used during spanning tree operation. The processing status is reset to its default value, once the spanning tree mode is changed. spanning-tree bpdu-receive { enabled | disabled }	Mode: Interface Config Mode (Physical Interface Mode)	1	**spanning-tree bpdu-receive enabled**	BPDU-Receive is disabled. Enter the command. Using the command **show spanning-tree detail** you can check if BPDU-Receive is enabled.	BPDU-Receive is enabled.
		2	spanning-tree bpdu-receive disabled	BPDU-Receive is enabled. Enter the command. Using the command **show spanning-tree detail** you can check if BPDU-Receive is disabled.	BPDU-Receive is disabled.

8.13 Spanning-Tree BDPU-Transmit

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the BPDU transmission status of a port. BPDUs are used to carry bridge related information that is used during spanning tree operation. The transmission status is reset to its default value, once the spanning tree mode is changed. spanning-tree bpdu-transmit { enabled | disabled }	Mode: Interface Config Mode (Physical Interface Mode)	1	**spanning-tree bpdu-transmit enabled**	BPDU-Transmit is disabled. Enter the command. Using the command **show spanning-tree detail** you can check if BPDU-Transmit is enabled.	BPDU-Transmit is enabled.
		2	**spanning-tree bpdu-transmit disabled**	BPDU-Transmit is enabled. Enter the command. Using the command **show spanning-tree detail** you can check if BPDU-Transmit is disabled.	BPDU-Transmit is disabled.

8.14 Spanning-Tree Loop-Guard

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the loop guard feature in a port. This feature prevents the alternative or root ports from becoming designated ports due to failure in a unidirectional link. This feature is useful if the neighbor bridge is faulty, that is, the bridge cannot send BPDUs but continues to send data traffic. The no form of this command disables the loop guard feature in the port. The loop guard feature is disabled, even if the spanning tree mode is changed. spanning-tree loop-guard no spanning-tree loop-guard	Mode: Interface Config Mode (Physical Interface Mode)	1	**spanning-tree loop-guard**	Loop Guard is disabled. Enter the command. Using the command **show spanning-tree detail** you can check if Loop Guard is enabled.	Loop Guard is enabled.
		2	**no spanning-tree loop-guard**	Loop Guard is enabled. Enter the command. Using the command **show spanning-tree detail** you can check if Loop Guard is disabled.	Loop Guard is disabled.

8.15 Show Spanning-Tree Summary

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays spanning tree related information available in the switch for the current STP enabled in the switch. The information contain priority, address and timer details for root and bridge, status of dynamic pathcost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type. show spanning-tree [{ summary | blockedports | pathcost method }] [switch <context_ name>]	Mode: Privileged EXEC Mode	1	**show spanning-tree summary**	Enter the command. You can check if currently used STP, applied path cost method and port details such as port ID, port role, port state and port status are displayed.	Currently used STP, applied path cost method and port details such as port ID, port role, port state and port status are displayed.
		2	**show spanning-tree blockedports**	Enter the command. You can check if the list of ports in blocked state and the total number of blocked ports are displayed.	List of ports in blocked state and the total number of blocked ports are displayed.
		3	show spanning-tree pathcost method	Enter the command. You can check if the port pathcost method configured for the switch is displayed.	Port pathcost method configured for the switch is displayed.

8.16 Show Spanning-Tree Detail

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold -count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and port fast features. show spanning-tree detail [switch <context_name>]	Mode: Privileged EXEC Mode	1	**show spanning-tree detail**	Enter the command. You can check if detailed spanning tree related information of the switch and all ports enabled in the switch are displayed.	Detailed spanning tree related information of the switch and all ports enabled in the switch are displayed.

8.17 Show Spanning-Tree Active

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays spanning tree related information available in the switch for the current STP enabled in the switch. The information contains priority, address and timer details for root and bridge, status of dynamic pathcost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type. show spanning-tree active [detail] [switch <context_ name>]	Mode: Privileged EXEC Mode	1	**show spanning-tree active**	Enter the command. You can check if spanning tree related information available in the switch for the current STP enabled in the switch is displayed.	Spanning tree related information available in the switch for the current STP enabled in the switch is displayed.

8.18 Show Spanning-Tree Interface

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the port related spanning tree information for the specified interface. The information contains port ID, port role, port state, port cost, port priority and link type. show spanning-tree interface <interface-type> <interface-id> [{ cost | priority | portfast | rootcost | restricted-role | restricted-tcn | state | stats | detail }]	Mode: Privileged EXEC Mode	1	**show spanning-tree interface gigabitethernet 0/3**	Enter the command. You can check if the port related spanning tree information for the specified type of interface is displayed.	Port related spanning tree information for the specified type of interface is displayed.
		2	**show spanning-tree interface gigabitethernet 0/3 cost**	Enter the command. You can check if the cost of the port or instances assigned to that port are displayed.	The cost of the port or instances assigned to that port are displayed.
		3	**show spanning-tree interface gigabitethernet 0/3 priority**	Enter the command. You can check if the priority of the port or instances assigned to that port are displayed.	The priority of the port or instances assigned to that port are displayed.
		4	**show spanning-tree interface gigabitethernet 0/3 portfast**	Enter the command. You can check if the status of the portfast feature for the port or instances assigned to that port are displayed.	The status of the portfast feature for the port or instances assigned to that port are displayed.
		5	show spanning-tree interface gigabitethernet 0/3 rootcost	Enter the command. You can check if the root cost of the port or instances assigned to that port are displayed.	The root cost of the port or instances assigned to that port are displayed.
		6	**show spanning-tree interface gigabitethernet 0/3 state**	Enter the command. You can check if the state of the port is displayed.	The state of the port is displayed.
		7	**show spanning-tree interface gigabitethernet 0/3 stats**	Enter the command. You can check if the port level spanning tree statistics information is displayed.	The port level spanning tree statistics information is displayed.

Command Description	Pre-Conditions	#	Step	Description	Result
		8	**show spanning-tree interface gigabitethernet 0/3 detail**	Enter the command. You can check if the detailed spanning tree related information for the port is displayed.	The detailed spanning tree related information for the port is displayed.
		9	**show spanning-tree interface gigabitethernet 0/3 restricted-role**	Enter the command. You can check if the status of the restricted role feature for the port is displayed.	The status of the restricted role feature for the port is displayed.
		10	**show spanning-tree interface gigabitethernet 0/3 restricted-tcn**	Enter the command. You can check if the status of the restricted TCN feature for the port is displayed.	The status of the restricted TCN feature for the port is displayed.

8.19 Show Spanning-Tree Root

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the spanning tree root information. The information contain root ID, root path cost, maximum age time, forward delay time and root port, for the RSTP. show spanning-tree root [{ address | cost | forward-time | id | max-age | port | priority | detail }] [switch <context_name>]	Mode: Privileged EXEC Mode	1	**show spanning-tree root**	Enter the command. You can check if the spanning tree root information is displayed.	The spanning tree root information is displayed.
		2	**show spanning-tree root address**	Enter the command. You can check if MAC address of the root bridge is displayed.	MAC address of the root bridge is displayed.
		3	**show spanning-tree root cost**	Enter the command. You can check if the cost of the root bridge is displayed.	The cost of the root bridge is displayed.
		4	show spanning-tree root forward-time	Enter the command. You can check if the forward delay time of the root bridge is displayed.	The forward delay time of the root bridge is displayed.
		5	**show spanning-tree root id**	Enter the command. You can check if the ID of the root bridge is displayed.	The ID of the root bridge is displayed.
		6	**show spanning-tree root max-age**	Enter the command. You can check if the maximum age time of the root bridge is displayed.	The maximum age time of the root bridge is displayed.
		7	**show spanning-tree root port**	Enter the command. You can check if the ID of the root port is displayed.	The ID of the root port is displayed.
		8	**show spanning-tree root priority**	Enter the command. You can check that the priority of the root bridge is displayed.	The priority of the root bridge is displayed.
		9	**show spanning-tree root detail**	Enter the command. You can check if the root priority, root address, root cost, root port, forward delay time and maximum age time are displayed.	The root priority, root address, root cost, root port, forward delay time and maximum age time are displayed.

8.20 Show Spanning-Tree Bridge

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the spanning tree bridge information. The information contain bridge ID, hello time, maximum age time, forward delay time and protocol enabled, for the RSTP. show spanning-tree bridge [{ address | forward-time | hello-time | id | max-age | protocol | priority | detail }] [switch <context_name>]	Mode: Privileged EXEC Mode	1	**show spanning-tree bridge**	Enter the command. You can check if the spanning tree bridge information is displayed.	The spanning tree bridge information is displayed.
		2	**show spanning-tree bridge address**	Enter the command. You can check if MAC address of the bridge is displayed.	MAC address of the bridge is displayed.
		3	**show spanning-tree bridge forward-time**	Enter the command. You can check if the forward delay time of the bridge is displayed.	The forward delay time of the bridge is displayed.
		4	show spanning-tree bridge hello-time	Enter the command. You can check if the hello time of the bridge is displayed.	The hello time of the bridge is displayed.
		5	**show spanning-tree bridge id**	Enter the command. You can check if the ID of the bridge is displayed.	The ID of the bridge is displayed.
		6	**show spanning-tree bridge max-age**	Enter the command. You can check if the maximum age time of the bridge is displayed.	The maximum age time of the bridge is displayed.
		7	**show spanning-tree bridge protocol**	Enter the command. You can check if the protocol currently enabled in the bridge is displayed.	The protocol currently enabled in the bridge is displayed.
		8	**show spanning-tree bridge priority**	Enter the command. You can check if the priority of the bridge is displayed.	The priority of the bridge is displayed.
		9	**show spanning-tree bridge detail**	Enter the command. You can check if the priority, address, maximum age time and forward delay time for the bridge are displayed.	The priority, address, maximum age time and forward delay time for the bridge are displayed.

9. VLAN

9.1 Shutdown VLAN

Command Description	Pre-Conditions	#	Step	Description	Result
This command shuts down the VLAN switching feature in the switch and releases all resources allocated to the VLAN feature. The no form of the command starts and enables VLAN switching feature in the switch. The resources required for the VLAN feature are also allocated to it. The VLAN feature allows you to logically segment a shared media LAN for forming virtual workgroups. shutdown vlan no shutdown vlan	Mode: Global Config Mode	1	**shutdown vlan**	VLAN Interface Mode, VLAN ID=2: VLAN switching feature is enabled. Enter the command. Using the command **show interfaces** you can check if VLAN switching feature (VLAN ID=2) is shut down.	VLAN switching feature (VLAN ID=2) is shutdown.
		2	**no shutdown vlan**	VLAN Interface Mode, VLAN ID=2: VLAN switching feature is shut down. Enter the command. Using the command **show interfaces** you can check if VLAN switching feature (VLAN ID=2) is started and enabled.	VLAN switching feature (VLAN ID=2) is started and enabled.

9.2 VLAN

Command Description	Pre-Conditions	#	Step	Description	Result
This command creates a VLAN in the HSS and enters into the config-VLAN mode in which VLAN specific configurations are done. This command directly enters into the config-VLAN mode for the specified VLAN, if the VLAN is already created. The created VLAN is identified using a unique VLAN ID whose value ranges between 1 and 4094. The no form of the command deletes the existing VLAN and its corresponding configurations. vlan <vlan-id(1-4094)> no vlan <vlan-id(1-4094)>	Mode: Global Config Mode	1	vlan 2	VLAN ID=2 doesn't exist. Enter the command. Activate the VLAN with **vlan active**. Using the command **show vlan** you can check if VLAN with ID=2 is created.	System is in the config-VLAN mode. VLAN with ID=2 is created.
		2	**no vlan 2**	VLAN ID=2 exists. Enter the command. Using the command **show vlan** you can check if VLAN with ID=2 is not available and deleted.	VLAN with ID=2 is not available.

9.3 VLAN Learning Mode

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the VLAN learning mode to be applied for all ports of the switch. This mode defines the forwarding database modes of operation to be implemented by the switch. vlan learning mode { ivl | svl } Hint: After changing this value you must reboot the switch.	Mode: Global Config Mode	1	**vlan learning mode ivl**	VLAN operational learning mode is Hybrid. Enter the command. Using the command **show vlan device info** you can check if VLAN operational learning mode is set to IVL.	VLAN operational learning mode is IVL.
		2	**vlan learning mode svl**	VLAN operational learning mode is IVL. Enter the command. Using the command **show vlan device info** you can check if VLAN operational learning mode is set to SVL.	VLAN operational learning mode is SVL.

9.4 Clear VLAN Statistics

Command Description	Pre-Conditions	#	Step	Description	Result
This command clears VLAN counters that maintain statistics information on a per VLAN basis. The counter is cleared for all available VLANs or for the specified VLAN. The statistics information contains number of unicast, broadcast and unknown unicast packets flooded. clear vlan statistics [vlan < vlan-id (1-4094)>]	Mode: Global Config Mode	1	**clear vlan statistics**	Enter the command. Check with the command **show vlan statistics** that counters for all available VLANs are cleared.	Counters for all available VLANs are cleared.
		2	**clear vlan statistics vlan 1**	VLAN ID=1 is started and enabled. Enter the command. Check with the command **show vlan statistics** that counters for VLAN ID=1 are cleared.	Counters for VLAN ID=1 are cleared.

9.5 Default VLAN ID

Command Description	Pre-Conditions	#	Step	Description	Result
Sets the default vlan id to be used after a reboot. default vlan id <count(1-4094)>	Mode: Global Config Mode	1	**default vlan id 10**	Sets the default VLAN ID to 10.	**show nvram** should show the configured default VLAN ID.

9.6 Ports

Command Description	Pre-Conditions	#	Step	Description	Result
This command statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN. The VLAN can also be activated using the vlan active command. The configuration defines the tagged and untagged member ports that are used for egress tagging of a VLAN at a port. The no form of the command deletes the specified port details for the VLAN. The member ports cannot be set empty for the VLAN, once the member ports details are configured for that VLAN. ports [add] ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/ab, 0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>]) [untagged <interfacetype> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,cd>] [pw <a,b,c-d>][all])] [forbidden <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>]] [name <vlan-name>] no ports [<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [all] [untagged ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [all])] [forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [all])] [name <vlan-name>]	Mode: Config-VLAN Mode	1	**ports gigabitethernet 0/1-8 untagged gigabitethernet 0/6 name VLAN3**	No ports are configured. Enter the command. Using the command **show vlan** you can check if member ports are set to 1-8, untagged ports are set to 6 and the name is set to VLAN3.	Member ports: 1-8 Untagged ports: 6 Forbidden ports: none Name: VLAN3

Command Description	Pre-Conditions	#	Step	Description	Result
		2	**ports add gigabitethernet 0/1-8 untagged gigabitethernet 0/5 name VLAN3_1**	Member ports: 1-8. Untagged ports: 6. Forbidden ports: none. Name: VLAN3. Enter the command. Using the command **show vlan** you can check if member ports are set to 1-8, untagged port 5 is added and the name is set to VLAN3_1.	Member ports: 1-8 Untagged ports: 5-6 Forbidden ports: none Name: VLAN3_1
		3	**ports add gigabitethernet 0/1-8 untagged gigabitethernet 0/7-8 name VLAN3_1**	Member ports: 1-8. Untagged ports: 5-6. Forbidden ports: none. Name: VLAN3_1. Enter the command. Using the command **show vlan** you can check if member ports are set to 1-8, untagged port 7-8 are added and the name is set to VLAN3_1.	Member ports: 1-8 Untagged ports: 5-8 Forbidden ports: none Name: VLAN3_1
		4	**ports gigabitethernet 0/1-4 name VLAN3_2**	No ports are configured. Enter the command. Using the command **show vlan** you can check if member ports are set to 1-4 and the name is set to VLAN3_2.	Member ports: 1-4 Untagged ports: none Forbidden ports: none Name: VLAN3_2
		5	**ports add gigabitethernet 0/5 name VLAN3_3**	Member ports: 1-4. Untagged ports: none. Forbidden ports: none. Name: VLAN3_2. Enter the command. Using the command **show vlan** you can check if member port 5 is added and the name is set to VLAN3_3.	Member ports: 1-5 Untagged ports: none Forbidden ports: none Name: VLAN3_3

Command Description	Pre-Conditions	#	Step	Description	Result
		6	**ports add gigabitethernet 0/6-7 name VLAN3_4**	Member ports: 1-5. Untagged ports: none. Forbidden ports: none. Name: VLAN3_3. Enter the command. Using the command **show vlan** you can check if member ports 6-7 are added and the name is set to VLAN3_4	Member ports: 1-7 Untagged ports: none Forbidden ports: none Name: VLAN3_4
		7	**no ports**	Member ports: 1-8. Untagged ports: 5-8. Forbidden ports: none. Name: VLAN3. Enter the command. Using the command **show vlan** you can check if all ports are set empty.	Member ports: Untagged ports: none Forbidden ports: none Name: VLAN3
		8	**no ports forbidden gigabitethernet 0/8**	Member ports: 1-6. Untagged ports: 5-6. Forbidden ports: 7-8. Name: VLAN3. Enter the command. Using the command **show vlan** you can check if forbidden port 8 is set empty.	Member ports: 1-6 Untagged ports: 5-6 Forbidden ports: 7 Name: VLAN3
		9	**no ports untagged gigabitethernet 0/6**	Member ports: 1-6. Untagged ports: 5-6. Forbidden ports: 7. Name: VLAN3. Enter the command. Using the command **show vlan** you can check if untagged port 6 is set empty.	Member ports: 1-6. Untagged ports: 5. Forbidden ports: 7. Name: VLAN3.
		10	**no ports gigabitethernet 0/1**	Member ports: 1-6. Untagged ports: 5. Forbidden ports: 7. Name: VLAN3. Enter the command. Using the command **show vlan** you can check if member port 1 is set empty.	Member ports: 2-6. Untagged ports: 5. Forbidden ports: 7. Name: VLAN3.

Command Description	Pre-Conditions	#	Step	Description	Result
		11	**no ports gigabitethernet 0/1 untagged gigabitethernet 0/6 forbidden gigabitethernet 0/8**	Member ports: 1-6. Untagged ports: 5-6. Forbidden ports: 7-8. Name: VLAN3. Enter the command. Using the command **show vlan** you can check if member port 1 is set empty, untagged port 6 is set empty, forbidden port 8 is set empty.	Member ports: 2-6. Untagged ports: 5. Forbidden ports: 7. Name: VLAN3.

9.7 VLAN Active

Command Description	Pre-Conditions	#	Step	Description	Result
This command activates a VLAN in the switch. The created VLANs should be active for further VLAN related configurations. The VLAN can also be activated using ports command. vlan active	Mode: Config-VLAN Mode	1	**vlan active**	The new VLAN is created. Enter the command. Using the command **show vlan** you can check if VLAN is activated.	VLAN is activated.

9.8 Unicast-MAC Learning

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables or disables unicast -MAC learning feature for a VLAN. The source MAC learning is not done in the switch if this feature is disabled for the VLAN. set unicast-mac learning { enable | disable | default }	Mode: Config-VLAN Mode	1	**set unicast-mac learning enable**	Enter the command. Using the command **show vlan learning params** you can check if unicast -MAC learning feature is enabled.	Unicast -MAC learning feature is enabled.
		2	**set unicast-mac learning disable**	Enter the command. Using the command **show vlan learning params** you can check if unicast -MAC learning feature is disabled.	Unicast -MAC learning feature is disabled.
		3	**set unicast-mac learning default**	Enter the command. Using the command **show vlan learning params** you can check if unicast -MAC learning feature is set to its default state.	Unicast -MAC learning feature is set to its default state.

9.9 Interface Range

Command Description	Pre-Conditions	#	Step	Description	Result
This command selects the range of physical interfaces and VLAN interfaces to be configured. The no form of the command selects the range of VLAN interfaces to be removed. This command is a complete standardized implementation of the existing command. This feature has been included in adherence to the Industry Standard CLI syntax. interface range ({ <interface-type> <slot/port-port>} {vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>}) no interface range vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>	Mode: Global Config Mode	1	**interface range gigabitethernet 0/1-5**	Enter the command. The system changes to mode “(hss(config-if-range)#”. Change the description for the selected ports with the command **description “ExampleString”**. Using the command **show interfaces description** you can check if the description for the selected ports is set to ExampleString.	Mode: config-if-range Description for the selected ports is ExampleString.
		2	**interface range vlan 1 - 5**	Enter the command with spaces. The system changes to mode “(config-if-range)”. Change the description for the selected VLAN range with the command **description “ExampleString”**. Using the command **show interfaces description** you can check if the description for the selected VLAN range 1-5 is set to ExampleString.	Mode: config-if-range Description for the selected VLAN range 1-5 is ExampleString.
		3	**no interface range vlan 2 - 5**	Enter the command with spaces. Using the command **show interfaces** or **show interfaces description** you can check if the selected vlan range 2-5 is removed.	Selected VLAN range 2-5 is removed.

9.10 Switchport Access VLAN

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the PVID (Port VLAN Identifier) on a port. This value ranges between 1 and 4094. The no form of this command sets the PVID to the default value on the port. This command is a complete standardized implementation of the existing command and operates similar to that of the command switchport pvid. This feature has been included in adherence to the Industry Standard CLI syntax. switchport access vlan <vlanid (1-4094)> no switchport access vlan	Mode: Interface Config Mode (Physical / Port Channel)	1	**switchport access vlan 4**	Gi0/8 is selected and shut down. VLAN 4 is created. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID is set to 4.	Port VLAN ID = 4
		2	**switchport access vlan 4**	Port Channel Interface (port 2) is selected and shut down. VLAN 4 is created. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID is set to 4.	Port VLAN ID = 4
		3	**switchport access vlan 4**	Gi0/8 is selected and shut down. VLAN 4 is not created. Enter the command. Using the command **show vlan port config** you can check if VLAN 4 is created and Port VLAN ID is set to 4.	VLAN 4 is created. Port VLAN ID = 4
		4	**switchport access vlan 4**	Port Channel Interface (port 2) is selected and shut down. VLAN 4 is not created. Enter the command. Using the command **show vlan port config** you can check if Access vlan 4 is created and Port VLAN ID is set to 4.	VLAN 4 is created. Port VLAN ID = 4

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**no switchport access vlan**	Gi0/8 is selected and shut down. Port VLAN ID = 10. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID is set to default value 1.	Port VLAN ID = 1
		6	**no switchport access vlan**	Port Channel Interface (port 2) is selected and shut down. Port VLAN ID = 10. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID is set to default value 1.	Port VLAN ID = 1

9.11 Switchport PVID

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the PVID on the specified port. The PVID represents the VLAN ID that is to be assigned to untagged frames or priority-tagged received on the port. The PVID is used for port-based VLAN type membership classification. The PVID configuration done is used based on the acceptable frame type of the port. The packets are processed against PVID. if the packets accepted at ingress is not having a tag. The no form of the command resets the PVID to the default value on the port. switchport pvid <vlan-id(1-4094)> no switchport pvid	Mode: Interface Config Mode	1	**switchport pvid 20**	Port Channel Interface. Port VLAN ID = 1. VLAN with ID=20 exists. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID is set to 20.	Port VLAN ID = 20.
		2	**switchport pvid 20**	Port Channel Interface. Port VLAN ID = 1. VLAN with ID=20 doesn't exist. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID stays unchanged (Port VLAN ID = 1).	Port VLAN ID = 1.
		3	**no switchport pvid**	Port Channel Interface. Port VLAN ID = 20. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID is set to default value 1.	Port VLAN ID = 1.

Command Description	Pre-Conditions	#	Step	Description	Result
		4	**switchport pvid 20**	Gigabitethernet Interface. Port VLAN ID = 1. VLAN with ID=20 exists. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID is set to 20.	Port VLAN ID = 20.
		5	**switchport pvid 20**	Gigabitethernet Interface. Port VLAN ID = 1. VLAN with ID=20 doesn't exist. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID stays unchanged (Port VLAN ID = 1).	Port VLAN ID = 1.
		6	**no switchport pvid**	Gigabitethernet Interface. Port VLAN ID = 20. Enter the command. Using the command **show vlan port config** you can check if Port VLAN ID is set to default value 1.	Port VLAN ID = 1.

9.12 Switchport Ingress-Filter

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables ingress filtering feature on the port. The ingress filtering is applied for the incoming frames received on the port. Only the incoming frames of the VLANs that have this port in its member list are accepted. This configuration does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames GMRP BPDU. The no form of the command disables ingress filtering feature on the port. All incoming frames received on the port are accepted. switchport ingress-filter no switchport ingress-filter	Mode: Interface Config Mode (Physical / Port Channel)	1	**switchport ingress-filter**	Gigabitethernet Interface. Port Ingress Filtering is disabled. Enter the command. Using the command **show vlan port config** you can check if Port Ingress Filtering is enabled.	Port Ingress Filtering is enabled.
		2	**no switchport ingress-filter**	Gigabitethernet Interface. Port Ingress Filtering is enabled. Enter the command. Using the command **show vlan port config** you can check if Port Ingress Filtering is disabled.	Port Ingress Filtering is disabled.
		3	**switchport ingress-filter**	Port Channel Interface. Port Ingress Filtering is disabled. Enter the command. Using the command **show vlan port config** you can check if Port Ingress Filtering is enabled.	Port Ingress Filtering is enabled.
		4	**no switchport ingress-filter**	Port Channel Interface. Port Ingress Filtering is enabled. Enter the command. Using the command **show vlan port config** you can check if Port Ingress Filtering is disabled.	Port Ingress Filtering is disabled.

9.13 Switchport Priority Default

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the default ingress user priority for a port. This priority is assigned to frames received on the port, that does not have a priority assigned to it. This priority value is useful only on media such as Ethernet, that does not support native user priority. This value ranges from 0 to 7. The value 0 represents the lowest priority and the value 7 represents the highest priority. The no form of the command resets the default ingress user priority for the port to its default value. switchport priority default <priority value(0-7)> no switchport priority default	Mode: Interface Config Mode (Physical / Port Channel)	1	**switchport priority default 4**	Physical / Port Channel Interface. Enter the command. Using the command **show vlan port config** you can check if Default Priority is set to 4.	Default Priority is 4.
		2	**no switchport priority default**	Physical / Port Channel Interface. Enter the command. Using the command **show vlan port config** you can check if Default Priority is set to default value 0.	Default Priority is 0.

9.14 Switchport Mode

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the mode of operation for a switch port. This mode defines the way of handling of traffic for VLANs. The no form of the command resets the mode of operation for the switch port to its default value. switchport mode { access | trunk | hybrid | { private-vlan {promiscuous | host } } | { dynamic { auto | desirable } } } no switchport mode	Mode: Interface Config Mode (Physical / Port Channel)	1	**switchport mode trunk**	Port is not an untagged port of a VLAN. Port Mode: Hybrid Enter the command. Using the command **show vlan port config** you can check if Port Mode is set to Trunk.	Port Mode: Trunk
		2	**switchport mode hybrid**	Port Mode: Host Enter the command. Using the command **show vlan port config** you can check if Port Mode is set to Hybrid.	Port Mode: Hybrid
		3	**switchport mode private-vlan promiscuous**	Port Mode: Host Enter the command. Using the command **show vlan port config** you can check if Port Mode is set to Promiscuous.	Port Mode: Promiscuous
		4	**switchport mode private-vlan host**	Port Mode: Promiscuous Enter the command. Using the command **show vlan port config** you can check if Port Mode is set to Host.	Port Mode: Host
		5	**no switchport mode**	Port Mode: Host Enter the command. Using the command **show vlan port config** you can check if Port Mode is set to default value Hybrid.	Port Mode: Hybrid

9.15 VLAN Max-Traffic-Class

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the maximum number of traffic classes supported on a port. The number of traffic classes supported depends on the hardware used, which can limit the number of traffic classes to a lower number. HARTING HSS supports eight traffic classes to handle priority traffic. Each traffic is assigned a traffic type based on the time sensitiveness of the traffic. This value ranges between 1 and 8. The no form of the command resets the maximum traffic class value on the port to its default value. vlan max-traffic-class <MAX Traffic class(1-8)> no vlan max-traffic-class	Mode: Interface Config Mode (Physical / Port Channel)	1	**vlan max-traffic-class 1**	Maximum number of traffic classes is 5. Enter the command. Using the command **show vlan traffic-classes** you can check if maximum number of traffic classes is set to 1.	Maximum number of traffic classes is 1.
		5	**no vlan max-traffic-class**	Enter the command. Using the command **show vlan traffic-classe**s you can check if maximum number of traffic classes is set to 8.	Maximum number of traffic classes is 8.

9.16 Show VLAN

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured. The information contains the member ports, untagged ports, forbidden ports, VLAN name and the status of that VLAN entry. show vlan [{brief | id <vlan-range> | summary | ascending}] [switch <context_name>]	Mode: Privileged EXEC Mode	1	**show vlan**	Enter the command. You can check that if VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured is displayed.	VLAN entry related information is displayed.
		2	**show vlan ascending**	Enter the command. You can check if the VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured is displayed in ascending order.	VLAN entry related information is displayed in ascending order.
		3	**show vlan brief**	Enter the command. You can check if the VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured is displayed.	VLAN entry related information is displayed.
		4	**show vlan summary**	Enter the command. You can check if only the total number of VLANs existing in the switch is displayed, the VLAN entry related information is not displayed.	Total number of VLANs existing in the switch is displayed. The VLAN entry related information is not displayed.
		5	**show vlan id 1**	Enter the command. You can check if the VLAN entry related information for specified VLAN ID=1 is displayed.	VLAN entry related information for specified VLAN ID=1 is displayed.
		6	**show vlan id 1-5**	Enter the command. You can check if the VLAN entry related information for specified VLANs ID=1 to 5 is displayed.	VLAN entry related information for specified VLANs ID=1 to 5 is displayed.

9.17 Show VLAN Device Info

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts. The information contains VLAN status, VLAN oper status, GVRP status, GMRP status, GVRP oper status, GMRP oper status, MAC-VLAN status, subnet-VLAN status, protocol -VLAN status, bridge mode of the switch, VLAN base bridge mode, VLAN traffic class status, VLAN learning mode, VLAN version number, maximum VLAN ID supported and maximum number of VLANs supported. show vlan device info [switch <context_name>]	Mode: Privileged EXEC Mode	1	**show vlan device info**	Enter the command. You can check if the VLAN global information that is applicable to all VLANs created in the switch is displayed.	VLAN global information that is applicable to all VLANs created in the switch is displayed.

9.18 Show VLAN Device Capabilities

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays only the list of VLAN features such as traffic class feature, supported in the switch / all contexts. show vlan device capabilities [switch <context_name>]	Mode: Privileged EXEC Mode	1	**show vlan device capabilities**	Enter the command. You can check if only the list of VLAN features such as traffic class feature, supported in the switch is displayed.	Only the list of VLAN features supported in the switch is displayed.

9.19 Show VLAN Traffic-Classes

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the evaluated user priority and traffic class mapping information of all interfaces available in the switch / all contexts. show vlan traffic-classes [{port <interface-type> <interface-id> | switch <context_name>}]	Mode: Privileged EXEC Mode	1	**show vlan traffic-classes**	Enter the command. You can check if the evaluated user priority and traffic class mapping information of all interfaces available in the switch are displayed.	The evaluated user priority and traffic class mapping information of all interfaces available in the switch are displayed.
		2	**show vlan traffic-classes port gigabitethernet 0/1**	Enter the command. You can check if the evaluated user priority and traffic class mapping information of the gigabitethernet interface are displayed.	The evaluated user priority and traffic class mapping information of the gigabitethernet interface are displayed.
		3	**show vlan traffic-classes port port-channel 1**	Port with ID=1 exists. Enter the command. You can check if the evaluated user priority and traffic class mapping information of the Port Channel Interface are displayed.	The evaluated user priority and traffic class mapping information of the Port Channel Interface are displayed.

9.20 Show VLAN Port Config

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the VLAN related port specific information for all interfaces available in the switch / all contexts. The information contains PVID, acceptable frame type, port mode, filtering utility criteria, default priority value and status of ingress filtering feature, GVRP module, GMRP module, restricted VLAN registration feature, restricted group registration feature, MAC-based VLAN membership, subnet-based VLAN membership, protocol-VLAN-based membership and port protected feature. show vlan port config [{port <interface-type> <interface-id> | switch <context_name>}]	Mode: Privileged EXEC Mode	1	**show vlan port config**	Enter the command. You can check if the VLAN related port specific information for all interfaces available in the switch is displayed.	The VLAN related port specific information for all interfaces available in the switch is displayed.
		2	**show vlan port config port gigabitethernet 0/1**	Enter the command. You can check if the VLAN related port specific information for the gigabitethernet interface is displayed.	The VLAN related port specific information for the gigabitethernet interface is displayed.
		3	**show vlan port config port port-channel 0/1**	Enter the command. You can check if the VLAN related port specific information for the Port Channel Interface is displayed.	The VLAN related port specific information for the Port Channel Interface is displayed.

9.21 Show VLAN Protocol-Group

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays all entries in the protocol group table. These entries contain protocol group information of the switch / all contexts. The information contain ID of a group, protocol assigned to the group, and frame type assigned to the group. show vlan protocols-group [switch <context_name>]	Mode: Privileged EXEC Mode	1	**show vlan protocols-group**	Enter the command. You can check if all entries in the protocol group table are displayed.	All entries in the protocol group table are displayed.

10. QoS / Diffserv

10.1 Shutdown QoS

Command Description	Pre-Conditions	#	Step	Description	Result
This command shuts down the QoS subsystem. The resources allocated to the QoS module are released back into the system. If the user does not require the services of the QoS module at run time uses this command to shut it down. The no form of the command starts the QoS subsystem. shutdown qos no shutdown qos	Mode: Global Config Mode	1	**shutdown qos**	System Control is set to Start. Enter the command. Using the command **show qos global info** you can check if System Control is set to Shutdown.	System Control is set to Shutdown.
		2	**no shutdown qos**	System Control is set to Shutdown. Enter the command. Using the command **show qos global info** you can check if System Control is set to Start.	System Control is set to Start.

10.2 QoS

Command Description	Pre-Conditions	#	Step	Description	Result
qos { enable | disable }	Mode: Global Config Mode	1	**qos enable**	QoS is started and disabled. Enter the command. Using the command **show qos global info** you can check if QoS is enabled.	QoS is enabled.
		2	**qos disable**	QoS is started and enabled. Enter the command. Using the command **show qos global info** you can check if QoS is disabled.	QoS is disabled.

10.3 QoS Scheduling Policy

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets packet scheduling algorithm for the device. qos scheduling policy { strict | wrr }	Mode: Global Config Mode	1	**qos scheduling policy strict**	Scheduling policy is Weighted Round Robin. Enter the command. Using the command **show qos scheduling policy** you can check if Scheduling policy is set to Strict Priority.	Scheduling policy is Strict Priority.
		2	**qos scheduling policy wrr**	Scheduling policy is Strict Priority. Enter the command. Using the command **show qos scheduling policy** you can check if Scheduling policy is set to Weighted Round Robin.	Scheduling policy is Weighted Round Robin.

10.4 QoS Match

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables VLAN priority /IP DSCP priority classification on this port. The no form of the command disables VLAN priority/IP DSCP priority classification on this port. qos match { vlanPri | ipDscp } no qos match { vlanPri | ipDscp }	Mode: Interface Config Mode	1	**qos match vlanPri**	Gi0/8 is selected. VLAN Priority is disabled on the port. Enter the command. Using the command **show qos port config** you can check if VLAN Priority is enabled on the port.	VLAN Priority is enabled.
		2	**no qos match vlanPri**	Gi0/8 is selected. Vlan Priority is enabled on the port. Enter the command. Using the command **show qos port config** you can check if VLAN Priority is disabled on the port.	VLAN Priority is disabled.
		3	**qos match ipDscp**	Gi0/8 is selected. IP DSCP Priority is disabled on the port. Enter the command. Using the command **show qos port config** you can check if IP DSCP Priority is enabled on the port.	IP DSCP Priority is enabled.
		4	**no qos match ipDscp**	Gi0/8 is selected. IP DSCP Priority is enabled on the port. Enter the command. Using the command **show qos port config** you can check if IP DSCP Priority is disabled on the port.	IP DSCP Priority is disabled.

10.5 QoS Override

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables VLAN ID/Source MAC/Destination MAC priority classification on this port. The no form of the command disables VLAN ID/ Source MAC/Destination MAC priority classification on this port. os { vlan-id | src-mac | dest-mac } override o qos { vlan-id | src-mac | dest-mac } override	Mode: Interface Config Mode	1	**qos vlan-id override**	Gi0/8 is selected. VLAN-ID priority is disabled. Enter the command. Using the command **show qos port override config** you can check if VLAN-ID priority is enabled.	VLAN-ID priority is enabled.
		2	**no qos vlan-id override**	Gi0/8 is selected. VLAN-ID priority is enabled. Enter the command. Using the command **show qos port override config** you can check if VLAN-ID priority is disabled.	VLAN-ID priority is disabled.
		3	**qos src-mac override**	Gi0/8 is selected. SRC-MAC priority is disabled. Enter the command. Using the command **show qos port override config** you can check if SRC-MAC priority is enabled.	SRC-MAC priority is enabled.
		4	**no qos src-mac override**	Gi0/8 is selected. SRC-MAC priority is enabled. Enter the command. Using the command **show qos port override config** you can check if SRC-MAC priority is disabled.	SRC-MAC priority is disabled.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**qos dest-mac override**	Gi0/8 is selected. DEST-MAC priority is disabled. Enter the command. Using the command **show qos port override config** you can check if DEST-MAC priority is enabled.	DEST-MAC priority is enabled.
		6	**no qos dest-mac override**	Gi0/8 is selected. DEST-MAC priority is enabled. Enter the command. Using the command **show qos port override config** you can check if DEST-MAC priority is disabled.	DEST-MAC priority is disabled.

10.6 QoS Tagifboth Match

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures which priority classification (VLAN priority or IP DSCP priority) to tag on the packet that carries both priorities is received on the port. qos tagifboth match { vlanPri | ipDscp }	Mode: Interface Config Mode	1	**qos tagifboth match vlanPri**	Gi0/8 is selected. IP DSCP priority is configured on the port. Enter the command. Using the command **show qos port config** you can check if VLAN priority is configured on the port.	VLAN priority is configured on the port.
		2	**qos tagifboth match ipDscp**	Gi0/8 is selected. VLAN priority is configured on the port. Enter the command. Using the command **show qos port config** you can check if IP DSCP priority is configured on the port.	IP DSCP priority is configured on the port.

10.7 Priority Map

Command Description	Pre-Conditions	#	Step	Description	Result
This command adds a priority map entry for mapping incoming priority to a regenerated priority. map [interface <iftype> <ifnum>] in-priority-type vlanPri in-priority <integer(0-7)> regen-priority <integer(0-7)>	Mode: Priority Map Config Mode	1	**map interface gigabitethernet 0/8 in-priority-type vlanPri in-priority 1 regen-priority 7**	Priority Map 1 is selected. InType is VLANPriority. InPriority is 0. Regen Priority is 0. Enter the command. Using the command **show priority-map** you can check if InPriority is set to 1 and Regen Priority to 7.	InType is VLANPriority. InPriority is 1. Regen Priority is 7.

10.8 Show QoS Global Info

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays QoS related global configurations such as system control and trace flag. show qos global info	Mode: Privileged EXEC Mode	1	**show qos global info**	Enter the command. You can check if QoS related global configurations such as system control and trace flag are displayed.	QoS related global configurations are displayed.

10.9 Show Priority Map

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the priority map entry such as PriorityMapId, IfIndex, InType, InPriority and RegenPriority. show priority-map [<priority-map-id(1-65535)>]	Mode: Privileged EXEC Mode	1	**show priority-map**	Enter the command. You can check if all available QoS priority map entries (PriorityMapId, IfIndex, InType, InPriority and RegenPriority) are displayed.	All available QoS priority map entries are displayed.
		2	**show priority-map 1**	Enter the command. You can check if QoS priority map entry with ID 1 (PriorityMapId, IfIndex, InType, InPriority and RegenPriority) is displayed.	QoS priority map entry with ID 1 is displayed.

10.10 Show Queue Map

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the configured queue map. show queue-map	Mode: Privileged EXEC Mode	1	**show queue-map**	Enter the command. You can check if configured queue map is displayed.	Configured queue map is displayed.

10.11 Show QoS Port Configuration

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the QoS port configuration. show qos port config [interface <iftype> <ifnum>]	Mode: Privileged EXEC Mode	1	**show qos port config**	Enter the command. You can check if QoS port configuration is displayed.	QoS port configuration is displayed.
		2	**show qos port config interface gigabitethernet 0/1**	Enter the command. You can check if QoS port configuration for the port Gi0/1 is displayed.	QoS port configuration for the port Gi0/8 is displayed.

10.12 Show QoS Port Override Configuration

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the QoS port override configuration. Information such as port, vlan id, source mac address and destination mac address are displayed. show qos port override config [interface <iftype> <ifnum>]	Mode: Privileged EXEC Mode	1	**show qos port override config**	Enter the command. You can check if the QoS port override configuration (port, vlan id, source mac address and destination mac address) is displayed.	QoS port override configuration is displayed.
		2	**show qos port override config interface gigabitethernet 0/1**	Enter the command. You can check if the QoS port override configuration (port, vlan id, source mac address and destination mac address) for the port Gi0/1 is displayed.	QoS port override configuration for the port Gi0/1 is displayed.

10.13 Show QoS Scheduling Policy

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the packet scheduling algorithm for the device. show qos scheduling policy	Mode: Privileged EXEC Mode	1	**show qos scheduling policy**	Enter the command. You can check if the packet scheduling algorithm for the device is displayed.	The packet scheduling algorithm for the device is displayed.

11. Rate Limiting - Broadcast Storm Filter

11.1 Storm-Control

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the storm control rate for broadcast, multicast and DLF packets and the no form of the command sets storm control rate for broadcast, multicast and DLF packets to the default value. storm-control { bcast | mcast_ bcast | dlf_mcast_bcast | all } level { 128K | 256K | 512K | 1M | 2M | 4M | 8M | 16M | 32M | 64M | 128M | 256M } no storm-control	Mode: Interface Config Mode	1	**storm-control bcast level 128K**	Gi0/8 is selected. Storm Control is disabled. Enter the command. Using the command **show interfaces gigabitethernet 0/8** you can check if Storm Control Type is set to BCAST and Ingress Storm Control Limit is 128K.	Storm Control Type is BCAST. Storm Control Limit is 128K.
		2	**storm-control mcast_bcast 1M**	Gi0/8 is selected. Storm Control is disabled. Enter the command. Using the command **show interfaces gigabitethernet 0/8** you can check if Storm Control Type is set to MCAST_ BCAST and Storm Control Limit is 1M.	Storm Control Type is MCAST_ BCAST. Storm Control Limit is 1M.
		3	**storm-control dlf_mcast_ bcast 512K**	Gi0/8 is selected. Storm Control is disabled. Enter the command. Using the command **show interfaces gigabitethernet 0/8** you can check if Storm Control Type is set to DLF_MCAST_BCAST and Storm Control Limit is 512K	Storm Control Type is DLF_MCAST_ BCAST. Storm Control Limit is 512K.
		4	**storm-control all 8M**	Gi0/8 is selected. Storm Control is disabled. Enter the command. Using the command **show interfaces gigabitethernet 0/8** you can check if Storm Control Type is set to All and Storm Control Limit is 8M.	Storm Control Type is All. Storm Control Limit is 8M.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**no storm-control**	Gi0/8 is selected. Storm Control Type is All. Storm Control Limit is 8M. Enter the command. Using the command **show interfaces gigabitethernet 0/8** you can check if Storm Control is disabled.	Storm Control is disabled.

11.2 Rate-Limit Output

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface and the no form of the command disables the rate limiting and burst size rate limiting on an egress port. rate-limit output [<rate-value>] [<burst-value>] no rate-limit output [rate-limit] [burst-limit] Rate-values: 128K | 256K | 512K | 1M | 2M | 4M | 8M | 16M | 32M | 64M | 128M | 256M	Mode: Interface Config Mode	1	**rate-limit output 512K**	Gi0/8 is selected. Egress Rate Limit is disabled. Enter the command. Using the command **show interfaces gigabitethernet 0/8** you can check if Egress Rate Limit is set to 512K.	Egress Rate Limit is 512K.
		2	**no rate-limit output**	Gi0/8 is selected. Egress Rate Limit is 512K. Enter the command. Using the command **show interfaces gigabitethernet 0/8** you can check if Rate limiting is disabled.	Rate limiting is disabled.

12. Port-Based Network Access Control (IEEE 802.1X) - PNAC

12.1 AAA Authentication Dot1x Default

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables the dot1x local authentication or RADIUS server or TACACS PLUS server-based remote authentication method for all ports. The actual authentication of the supplicant happens at the authentication server. The no form of the command disables dot1x in the switch. aaa authentication dot1x default { group { radius | tacacsplus | tacacs+} | local } no aaa authentication dot1x default	Mode: Global Config Mode	1	**aaa authentication dot1x default group radius**	Dot1x is enabled in the switch. Dot1x Authentication Method: Local. Enter the command. Using the command **show dot1x** you can check if Dot1x Authentication Method is set to RADIUS.	Dot1x Authentication Method: RADIUS.
		2	**aaa authentication dot1x default group tacacs+**	Dot1x is enabled in the switch. Dot1x Authentication Method: RADIUS. Enter the command. Using the command **show dot1x** you can check if Dot1x Authentication Method is set to TACACS PLUS.	Dot1x Authentication Method: TACACS PLUS.
		3	**aaa authentication dot1x default group tacacsplus**	Dot1x is enabled in the switch. Dot1x Authentication Method: RADIUS. Enter the command. Using the command **show dot1x** you can check if Dot1x Authentication Method is set to TACACS PLUS.	Dot1x Authentication Method: TACACS PLUS.

Command Description	Pre-Conditions	#	Step	Description	Result
		4	**aaa authentication dot1x default local**	Dot1x is enabled in the switch. Dot1x Authentication Method: TACACS PLUS. Enter the command. Using the command **show dot1x** you can check if Dot1x Authentication Method is set to Local.	Dot1x Authentication Method: Local.
		5	**no aaa authentication dot1x default**	Dot1x is enabled in the switch. Dot1x Authentication Method: Local. Enter the command. Using the command **show dot1x** you can check if Dot1x is disabled in the switch.	Dot1x is disabled in the switch.

12.2 Dot1x Local-Database

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures dot1x authentication server local database with user name and password. The no form of the command deletes an entry from the dot1x authentication server database. dot1x local-database <username> password <password> permission {allow | deny} [<auth-timeout (value(1-7200))>] [interface <interface-type> <interface-list>] no dot1x local-database <username>	Mode: Global Config Mode	1	**dot1x local-database admin1 password admin1 permission allow auth-timeout 6000**	User name "admin1" is not configured. Enter the command. Using the command **show dot1x** local-database you can check if the new entry with user name "admin1", permission "allow" and timeout "6000" is created.	The new entry with user name "admin1", permission "allow" and timeout "6000" is created.
		2	**dot1x local-database admin1 password admin1 permission allow auth-timeout 6000 interface gigabitethernet 0/1**	User name "admin1" is not configured. Enter the command. Using the command **show dot1x** local-database you can check if the new entry with user name "admin1", permission "allow", timeout "6000" and port "Gi0/1" is created.	The new entry with user name "admin1", permission "allow", timeout "6000" and port "Gi0/1" is created.
		3	**no dot1x local-database admin1**	User name "admin1" is configured. Enter the command. Using the command **show dot1x** local-database you can check if the entry with user name "admin1" is deleted.	The entry with user name "admin1" is deleted.

12.3 NAS-ID

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the dot1x network access server id. Network Access Server Identifier is set in the RADIUS packets sent to the Remote Authentication Server Maximum length of the string is 16. set nas-id <identifier>	Mode: Global Config Mode	1	**set nas-id BBBBBB**	Remote authentication server is RADIUS. NAS ID: RADIUS Server. Enter the command. Using the command **show dot1x** you can check if NAS ID is set to BBBBBB.	NAS ID: BBBBBB.
		2	**set nas-id CCCCCC**	Remote authentication server is Tacacs. Nas Id: BBBBBB. Enter the command. Using the command **show dot1x** you can check if NAS ID is set to CCCCCC.	NAS ID: CCCCCC.

12.4 Dot1x System-Auth-Control

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables dot1x in the switch. The dot1x is an authentication mechanism. It acts as mediator between the authentication server and the supplicant (client). If the client accesses the protected resources, it contacts the authenticator with EAPOL frames. The no form of this command disables dot1x in the switch. dot1x system-auth-control no dot1x system-auth-control	Mode: Global Config Mode	1	**dot1x system-auth-control**	Dot1x is disabled in the switch. Enter the command. Using the command **show dot1x** you can check if Sysauthcontrol and Module Oper Status are set to enabled.	Sysauthcontrol: Enabled, Module Oper Status: Enabled.
		2	**no dot1x system-auth-control**	Dot1x is enabled in the switch. Enter the command. Using the command **show dot1x** you can check if Sysauthcontrol and Module Oper Status are set to disabled.	Sysauthcontrol: Disabled, Module Oper Status: Disabled.

12.5 Shutdown Dot1x

Command Description	Pre-Conditions	#	Step	Description	Result
This command shuts down dot1x feature. By shutting down the dot1x feature, the supplicant - authenticator-authentication server architecture is dissolved. The data transport and authentication are directly governed by the authentication server/server. If shut down, all resources acquired by dot1x module are released to the system. The no form of the command starts and enables dot1 xshutdown dot1 xno shutdown dot1x	Mode: Global Config Mode	1	**shutdown dot1x**	Dot1x is not shut down. Enter the command. Using the command **show dot1x** you can check if Dot1x is shut down.	Dot1x is shutdown.
		2	**no shutdown dot1x**	Dot1x is shut down. Enter the command. Using the command **show dot1x** you can check if Dot1x is not shut down.	Dot1x is not shutdown.

12.6 Dot1x Default

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures dot1x with default values for this port. The previous configurations on this port are reset to the default values. These details are not displayed but are the basic settings for a port. dot1x default	Mode: Interface Config Mode	1	**dot1x default**	Gi0/1 is selected. Dot1x Authentication Mode is Mac-based. Port Control is Auto. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Dot1x is configured with default values for the port Gi0/1.	Dot1x is configured with default values for the port Gi0/1: Authentication Mode is Port-based, Port Control is Force Authorized.

12.7 Dot1x Initialize

Command Description	Pre-Conditions	#	Step	Description	Result
Initializes the state machines and sets up the environment for fresh authentication. This initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. dot1x initialize [interface <interface-type> <interface-id>]	Mode: Privileged EXEC Mode Dot1X is configured for at least one port.	1	**dot1x initialize interface fastethernet 0/1**	Reinitialises the dot1x protocol on port 0/1. The attached host is forced to authenticate.	Any hosts that cannot re-authenticate are denied access to the network.

12.8 Dot1x Init-Session

Command Description	Pre-Conditions	#	Step	Description	Result
Initiates dot1x authentication session for the given MAC address of the supplicant, which sends EAPOL frames to the authenticator. The session is initiated when the supplicant is authorized by the remote server. dot1x init-session <supp addr - aa.aa.aa.aa.aa.aa>	Mode: Global Config Mode Dot1x is configured.	1	**dot1x init-session 00:01:02:03:04:05**	Initiates dot1x authentication for the host with given MAC address.	The host is enabled to access the protected network.

12.9 Dot1x Max-Start

Command Description	Pre-Conditions	#	Step	Description	Result
Sets the maximum number of EAPOL retries. dot1x max-start <count(1-65535)> no dot1x max-start	Mode: Interface Config Mode	1	**dot1x max-start 2**	Sets the number of allowed authentication retries to 2.	Any host that cannot authenticate with three attempts, will not be allowed to authenticate.
		2	**no dot1x max-start**	Sets the number of allowed authentication retries to default.	

12.10 Dot1x Max-Req

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client by the authenticator before restarting authentication process. The count value ranges between 1 and 10. The no form of the command sets the maximum number of EAP retries to the client to default value. dot1x max-req <count(1-10)> no dot1x max-req	Mode: Interface Config Mode	1	**dot1x max-req 10**	Gi0/8 is selected. MaxReq: 2 Enter the command. Using the command **show dot1x interface gigabitethernet 0/8** you can check if MaxReq is set to 10.	MaxReq: 10.
		2	**no dot1x max-req**	Gi0/8 is selected. MaxReq: 10 Enter the command. Using the command **show dot1x interface gigabitethernet 0/8** you can check if MaxReq is set to 2.	MaxReq: 2

12.11 Dot1x Reauthentication

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables periodic re-authentication from authenticator to client. The periodic reauthentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually. The no form of the command disables periodic re-authentication from authenticator to client. dot1x reauthentication dot1x re-authenticate [interface <interface-type><interface-id>] no dot1x reauthentication	Mode: Interface Config Mode	1	**dot1x reauthentication**	Gi0/1 is selected. Dot1x Port Control: Auto. MaxReq: Disabled. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if MaxReq is set to Enabled.	MaxReq: Enabled.
		2	**no dot1x reauthentication**	Gi0/1 is selected. Dot1x Port Control: Auto. MaxReq: Enabled. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if MaxReq is set to Disabled.	MaxReq: Disabled.

12.12 Dot1x Init Session-Reauthentication

Command Description	Pre-Conditions	#	Step	Description	Result
Initiates dot1x re-authentication. If the supplicant exceeds the time limit for accessing the protected network, the supplicant is forced to re-authenticate. Re-authentication is done manually by configuring the MAC of the supplicant. dot1x init session-reauth <supp addr - aa.aa.aa.aa.aa.aa>	Mode: Global Config Mode	1	**dot1x init session-reauth 00:01:02:03:04:05**	Dot1x Reauthentication is configured. Reauthenticates the supplicant with the MAC-address 00:01:02:03:04:05	Allows the host with the configured mac address to access the network for the duration that was configured using dot1x timeout.

12.13 Dot1x Timeout

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the dot1x timers. The timer module manages timers, creates memory pool for timers, creates timer list, starts and stops timer. It provides handlers to respective expired timers. The no form of the command sets the dot1x timers to the default values. dot1x timeout { quiet-period <value (0-65535)> | { reauth-period | servertimeout | supp-timeout | tx-period | start-period | held-period | auth-period } <value (1-65535)> } no dot1x timeout { quiet-period | reauth-period | server-timeout | supp-timeout | tx-period | start-period | held-period | auth-period }	Mode: Interface Config Mode	1	**dot1x timeout quiet-period 10000**	QuietPeriod: 60. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if QuietPeriod is set to 10000.	QuietPeriod: 10000.
		2	**no dot1x timeout quiet-period**	QuietPeriod: 10000. Enter the command. Using the command show dot1x interface **gigabitethernet 0/1** you can check if QuietPeriod is set to default value 60.	QuietPeriod: 60.
		3	**dot1x timeout reauth-period 10000**	ReAuthPeriod: 3600 Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if ReAuthPeriod is set to 10000.	ReAuthPeriod: 10000.
		4	**no dot1x timeout reauth-period**	ReAuthPeriod: 10000. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if ReAuthPeriod is set to default value 3600.	ReAuthPeriod: 3600.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**dot1x timeout server-timeout 10000**	ServerTimeout: 30. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if ServerTimeout is set to 10000.	ServerTimeout: 10000.
		6	**no dot1x timeout server-timeout**	ServerTimeout: 10000. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if ServerTimeout is set to default value 30.	ServerTimeout: 30.
		7	**dot1x timeout supp-timeout 10000**	SuppTimeout: 30 Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if SuppTimeout is set to 10000.	SuppTimeout: 10000.
		8	**no dot1x timeout supp-timeout**	SuppTimeout: 10000. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if SuppTimeout is set to default value 30.	SuppTimeout: 30.
		9	**dot1x timeout tx-period 10000**	Tx Period: 30. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Tx Period is set to 10000.	Tx Period: 10000.
		10	**no dot1x timeout tx-period**	Tx Period: 10000. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Tx Period is set to default value 30.	Tx Period: 30.

Command Description	Pre-Conditions	#	Step	Description	Result
		11	**dot1x timeout start-period 10000**	Access Control: Active. Start Period: 30 Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Start Period is set to 10000.	Start Period: 10000.
		12	**no dot1x timeout start-period**	Access Control: Active. Start Period: 10000. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Start Period is set to default value 30.	Start Period: 30.
		13	**dot1x timeout held-period 10000**	Access Control: Active. Held Period: 60 Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Held Period is set to 10000.	Held Period: 10000.
		14	**no dot1x timeout held-period**	Access Control: Active. Held Period: 10000. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Held Period is set to default value 60.	Held Period: 30.
		15	**dot1x timeout auth-period 10000**	Access Control: Active. Auth Period: 30 Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Auth Period is set to 10000.	Auth Period: 10000.
		16	**no dot1x timeout auth-period**	Access Control: Active. Auth Period: 10000. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Auth Period is set to default value 30.	Auth Period: 30.

12.14 Dot1x Port-Control

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the authenticator port control parameter. The dot1x exercises port-based authentication to increase the security of the network. The different modes employed to the ports offer varied access levels. The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports The no form of the command sets the authenticator port control state to force authorized. dot1x port-control { auto | force-authorized | force-unauthorized } no dot1x port-control	Mode: Interface Config Mode	1	**dot1x port-control auto**	Gi0/1 is selected. Port Control: Force Authorized. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Port Control is set to Auto.	Port Control: Auto.
		2	**dot1x port-control force-authorized**	Gi0/1 is selected. Port Control: Auto. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Port Control is set to Force Authorized.	Port Control: Force Authorized.
		3	**dot1x port-control force-unauthorized**	Gi0/1 is selected. Port Control: Force Authorized. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Port Control is set to Force Unauthorized.	Port Control: Force Un-Authorized.
		4	**no dot1x port-control**	Gi0/1 is selected. Port Control: Force Un-Authorized. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if Port Control is set to Force Authorized.	Port Control: Force Authorized.

12.15 Dot1x Access-Control

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the supplicant access control. The port is operating as both Supplicant and Authenticator if the setting is needed to apply the Supplicant authorization state. The no form of the command sets the access control to inactive. dot1x access-control { active | inactive } no dot1x access-control	Mode: Interface Config Mode	1	**dot1x access-control active**	Gi0/1 is selected. AccessControl: Inactive. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if AccessControl is set to Active.	AccessControl: Active.
		2	**dot1x access-control inactive**	Gi0/1 is selected. AccessControl: Active. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if AccessControl is set to Inactive.	AccessControl: Inactive.
		3	**no dot1x access-control**	Gi0/1 is selected. AccessControl: Active. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if AccessControl is set to Inactive.	AccessControl: Inactive.

12.16 Dot1x Control-Direction

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures port control direction. The switch port authenticates incoming packets and outgoing packets. The direction can be configured manually by selecting either in or both. By default the value is both. The no form of the command sets the authenticator port control direction to both dot1x control-direction { in | both } no dot1x control-direction	Mode: Interface Config Mode	1	**dot1x control-direction in**	Gi0/8 is selected. AdminControlDirection: Both. Enter the command. Using the command **show dot1x interface gigabitethernet 0/8** you can check if AdminControlDirection is set to In.	AdminControl-Direction: In.
		2	**dot1x control-direction both**	Gi0/8 is selected. AdminControlDirection: In. Enter the command. Using the command **show dot1x interface gigabitethernet 0/8** you can check if AdminControlDirection is set to Both.	AdminControl-Direction: Both.
		3	**no dot1x control-direction**	Gi0/8 is selected. AdminControlDirection: In. Enter the command. Using the command **show dot1x interface gigabitethernet 0/8** you can check if AdminControlDirection is set to Both.	AdminControl-Direction: Both.

12.17 Dot1x Auth-Mode

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the authentication mode of a port as either port -based (which is also known as multi-host) or MAC-based (which is also known as single-host). Port-based authentication has different modes of authentication. MAC-based authentication allows secured mac addresses to pass through the port. Non secure mac addresses are dropped. The no form of the command configures the port authentication mode to its default values. dot1x auth-mode { port-based | mac-based } no dot1x auth-mode	Mode: Interface Config Mode	1	**dot1x auth-mode port-based**	Gi0/1 is selected. Port Control: Auto. AuthMode: MAC-based. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if AuthMode is set to Port-based.	AuthMode: Port-based.
		2	**dot1x auth-mode mac-based**	Gi0/1 is selected. Port Control: Auto. AuthMode: Port-based. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if AuthMode is set to MAC-based.	AuthMode: MAC-based.
		3	**no dot1x auth-mode**	Gi0/1 is selected. Port Control: Auto. AuthMode: MAC-based. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if AuthMode is set to Port-based.	AuthMode: Port-based.

12.18 Dot1x Host-Mode

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the port authentication mode of a port as either multi-host (which is also known as port-based) or single-host (which is also known as MAC-based). Multi host authentication has different modes of authentication. Single host authentication allows secured mac addresses to pass through the port. Non secure mac addresses are dropped. This command is a standardized implementation of the existing command; dot1x auth-mode. It operates similar to the existing command. dot1x host-mode { multi-host | single-host }	Mode: Interface Config Mode	1	**dot1x host-mode multi-host**	Gi0/1 is selected. Port Control: Auto. AuthMode: MAC-based. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if AuthMode is set to Port-based.	AuthMode: Port-based.
		2	**dot1x host-mode single-host**	Gi0/1 is selected. Port Control: Auto. AuthMode: Port-based. Enter the command. Using the command **show dot1x interface gigabitethernet 0/1** you can check if AuthMode is set to MAC-based.	AuthMode: MAC-based.

12.19 Show Dot1x

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays dot1x information. The configured information can be viewed by running this show command. Use the show command to ensure that the port is configured as desired. show dot1x [{ interface <interface-type> <interface-id> | statistics interface <interface-type> <interface-id> | supplicant-statistics interface <interfacetype> <interface-id>|local-database | mac-info [address <aa.aa.aa.aa.aa.aa>] | mac-statistics [address <aa.aa.aa.aa.aa.aa>] | all }]	Mode: Privileged EXEC Mode	1	**show dot1x**	Enter the command. You can check if dot1x information is displayed.	Dot1x information is displayed.
		2	**show dot1x all**	Enter the command. You can check if dot1x status for all interfaces is displayed.	Dot1x status for all interfaces is displayed.
		3	**show dot1x interface gigabitethernet 0/8**	Enter the command. You can check if dot1x status for the specified interface (Gi0/8) is displayed.	Dot1x status for the specified interface (Gi0/8) is displayed.
		4	**show dot1x local-database**	Enter the command. You can check if dot1x authentication server database with user name and password is displayed.	Dot1x authentication server database with user name and password is displayed.
		5	**show dot1x supplicant-statistics interface gigabitethernet 0/8**	Enter the command. You can check if dot1x supplicant statistics parameters for the specified interface are displayed.	Dot1x supplicant statistics parameters for the specified interface are displayed.
		6	**show dot1x statistics interface gigabitethernet 0/8**	Enter the command. You can check if dot1x authenticator port statistics parameters for the specified interface are displayed.	Dot1x authenticator port statistics parameters for the specified interface are displayed.

Command Description	Pre-Conditions	#	Step	Description	Result
		7	**show dot1x mac-info**	Enter the command. You can check if dot1x MAC session is displayed.	Dot1x MAC session is displayed.
		8	**show dot1x mac-statistics**	Enter the command. You can check if dot1x MAC statistic is displayed.	Dot1x MAC statistic is displayed.

13. RADIUS

13.1 RADIUS-Server Host

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the RADIUS client with the parameters (host, timeout, key, retransmit).The no form of the command deletes RADIUS server configuration. radius-server host { ipv4-address | host-name } [auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>] [retransmit <1-254>] [key <secret-key-string>] [primary] no radius-server host { ipv4-address | host-name } [primary]	Mode: Global Config Mode	1	**radius-server host 10.0.0.2 key pass**	Enter the command. Using the command **show radius server** you can check if the RADIUS client with the parameters (host, timeout, key, retransmit) is configured.	The RADIUS client with the parameters (host, timeout, key, retransmit) is configured.
		2	**radius-server host 10.0.0.2 timeout 20 key pass**	Enter the command. Using the command **show radius server** you can check if Response Time is set to 20.	Response Time is 20.
		3	**radius-server host 10.0.0.2 retransmit 50 key pass**	Enter the command. Using the command **show radius server** you can check if Maximum Retransmission is set to 50.	Maximum Retransmission is 50.
		4	**radius-server host 10.0.0.2 acct-port 2 key pass**	Enter the command. Using the command **show radius server** that Accounting Port is set to 2.	Accounting Port is 2.
		5	**radius-server host 10.0.0.2 auth-port 3 key pass**	Enter the command. Using the command **show radius server** you can check if Authentication Port is set to 3.	Authentication Port is 3.
		6	**no radius-server host 10.0.0.2**	Enter the command. Using the command **show radius server** you can check if RADIUS server configuration is deleted.	RADIUS server configuration is deleted.

13.2 Show RADIUS Server

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays RADIUS server Host information which contains, Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port. show radius server [{ <ucast_ addr> | <string> }]	Mode: Privileged EXEC Mode	1	**show radius server**	Enter the command. You can check if RADIUS server Host information such as Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port is displayed.	RADIUS server Host information is displayed.

13.3 Show RADIUS Statistics

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation. show radius statistics	Mode: Privileged EXEC Mode	1	**show radius statistics**	Enter the command. You can check if RADIUS Server Statistics for the data transfer between server and the client from the time of initiation are displayed.	RADIUS Server Statistics are displayed.

14. Link Aggregation (LA)

14.1 Set Port-Channel

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the admin status of LA in the switch. The LA feature allows you to aggregate individual point -to-point links into a port channel group. Thus, the capacity and availability of the communication channel between devices are increased by using the existing interface technology. set port-channel { enable | disable }	Mode: Global Config Mode	1	**set port-channel enable**	LA is not shut down. Port Channel Module Admin Status is disabled. Enter the command. Using the command **show etherchannel** you can check if Port Channel Module Admin Status is set to enabled.	Port Channel Module Admin Status is enabled.
		2	**set port-channel disable**	LA is not shut down. Port Channel Module Admin Status is enabled. Enter the command. Using the command show etherchannel you can check if Port Channel Module Admin Status is set to disabled.	Port Channel Module Admin Status is disabled.

14.2 Shutdown Port-Channel

Command Description	Pre-Conditions	#	Step	Description	Result
This command shuts down LA feature in the switch and releases all resources allocated to the LA feature. The no form of the command starts and enables LA feature in the switch, and allocates required memory to the LA module. The LA feature is available only if the LA is enabled in the switch. LA feature allows to aggregate individual point-to-point links into a port channel group, thus the capacity and availability of the communication channel between devices are increased by using the existing interface technology. shutdown port-channel no shutdown port-channel	Mode: Global Config Mode	1	**shutdown port-channel**	LA is not shut down. Enter the command. Using the command **show etherchannel** you can check if LA is shut down.	LA is shutdown.
		2	**no shutdown port-channel**	LA is shut down. Enter the command. Using the command **show etherchannel** you can check if LA is not shut down.	LA is not shutdown.

14.3 Channel-Protocol

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables link aggregation in the switch. This command is a standardized implementation of the existing command; set port channel. It operates similar to the existing command. The no form of the command disables link aggregation in the switch. channel-protocol { lacp | pagp } no channel-protocol	Mode: Global Config Mode	1	**channel-protocol lacp**	LA is not shut down. Port Channel Module Admin Status is disabled. Enter the command. Using the command **show etherchannel** you can check if Port Channel Module Admin Status is set to enabled.	Port Channel Module Admin Status is enabled.
		2	**no channel-protocol**	LA is not shut down. Port Channel Module Admin Status is enabled. Using the command **show etherchannel** you can check if Port Channel Module Admin Status is set to disabled.	Port Channel Module Admin Status is disabled.

14.4 LACP System-Priority

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the LACP priority associated with actor's system ID. This priority value ranges between 0 and 65535. The switch with the lowest LACP decides the standby and active links in the LA. The no form of the command resets the LACP priority to its default value. lacp system-priority <0-65535> no lacp system-priority	Mode: Global Config Mode	1	**lacp system-priority 30000**	LACP System Priority: 32768. Enter the command. Using the command **show etherchannel** you can check if LACP System Priority is set to 30000.	LACP System Priority is 30000.
		2	**no lacp system-priority**	LACP System Priority: 30000. Enter the command. Using the command **show etherchannel** you can check if LACP System Priority is set to 32768.	LACP System Priority is 32768.

14.5 LACP System-Identifier

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the global LACP system ID. The system ID denotes a 6-octet unicast MAC address value that is used as a unique identifier for the switch containing the aggregator. The no form of the command resets the global LACP System ID to its default value. lacp system-identifier <aa:aa:aa:aa:aa:aa> no lacp system-identifier	Mode: Global Config Mode	1	**lacp system-identifier 00:11:22:33:44:99**	LA functionality is started and enabled. Port-channel System Identifier: default value. Enter the command. Using the command **show etherchannel** you can check if Port-channel System Identifier is set to 00:11:22:33:44:99.	Port-channel System Identifier is 00:11:22:33:44:99.
		2	**no lacp system-identifier**	LA functionality is started and enabled. Port-channel System Identifier: 00:11:22:33:44:99. Using the command **show etherchannel** you can check if Port-channel System Identifier is set to default value.	Port-channel System Identifier is set to default value.

14.6 LACP Port-Priority

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the LACP port priority. This port priority is used in combination with LACP port identifier during the identification of best ports in a port channel. If the number of ports in the aggregation exceeds the maximum number supported by the hardware the priority determines whether a link is active or in the standby mode. The links with lower priority become active links. Their value ranges between 0 and 65535. The no form of the command resets the LACP port priority to its default value. lacp port-priority <0-65535> no lacp port-priority	Mode: Interface Config Mode (Physical Interface Mode)	1	**lacp port-priority 20000**	Gi0/8 is selected. LACP Port Priority: 128. Enter the command. Using the command **show interfaces gigabitethernet 0/8 etherchannel** you can check if LACP Port Priority is set to 20000.	LACP Port Priority: 20000.
		2	**no lacp port-priority**	Gi0/8 is selected. LACP Port Priority: 20000. Enter the command. Using the command **show interfaces gigabitethernet 0/8 etherchannel** you can check if LACP Port Priority is set to 128.	LACP Port Priority 128.

14.7 LACP Port-Identifier

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the LACP actor admin port ID to be filled in the LACP PDUs. This value represents the concerned aggregation port. This value ranges from 1 to 65535. The maximum limit depends on the board. For Example, if the board has only 24 ports, than the maximum value will be 24 only. That is the value ranges from 1 to 24. lacp port-identifier <1-65535>	Mode: Interface Config Mode (Physical Interface Mode)	1	**lacp port-identifier 10**	LACP Admin Port: 4. Enter the command. Using the command **show interfaces gigabitethernet 0/8 etherchannel** you can check if LACP Admin Port is set to 10.	LACP Admin Port: 10.

14.8 Channel-Group

Command Description	Pre-Conditions	#	Step	Description	Result
This command adds the port as a member of the specified port channel that is already created in the switch. The no form of the command deletes the aggregation of the port from all port channels. channel-group <channel-group-number(1-65535)> mode { auto [non-silent] | desirable [non-silent] | on | active | passive } no channel-group	Mode: Interface Config Mode (Physical Interface Mode)	1	**channel-group 119 mode active**	Port Channel with ID 119 is created. Port Gi0/8 is not added to the Port Channel with ID 119. Port Gi0/8 is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/8 etherchannel** you can check if: - port Gi0/8 is added to the specified Port Channel with ID 119, - Mode is set to Active, - LACP Activity is set to Active.	The port Gi0/8 is added to the specified Port Channel with ID 119. Mode is Active. LACP Activity is Active.
		2	**channel-group 119 mode on**	Port Channel with ID 119 is created. Port Gi0/8 is not added to the Port Channel with ID 119. Port Gi0/8 is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/8 etherchannel** you can check if: - port Gi0/8 is added to the specified Port Channel with ID 119, - Mode is set to On, - LACP Activity is set to Passive.	The port Gi0/8 is added to the specified Port Channel with ID 119. Mode is On. LACP Activity is Passive.

Command Description	Pre-Conditions	#	Step	Description	Result
		3	**channel-group 119 mode passive**	Port Channel with ID 119 is created. Port Gi0/8 is not added to the Port Channel with ID 119. Port Gi0/8 is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/8 etherchannel** you can check if: - port Gi0/8 is added to the specified Port Channel with ID 119, - Mode is set to Active, - LACP Activity is set to Passive.	The port Gi0/8 is added to the specified Port Channel with ID 119. Mode is Active. LACP Activity is Passive.
		4	**no channel-group**	Port Gi0/8 is added to the Port Channel with ID 119. Gi0/8 is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/8 etherchannel** you can check if the port Gi0/8 is deleted from the Port Channel with ID 119.	The port Gi0/8 is deleted from the Port Channel with ID 119.

14.9 LACP Wait-Time

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the LACP wait-time for an interface. The wait time represent the time (in seconds) till which the port waits before entering into aggregation after receiving partner information (that is, this represents the time taken to attach to the port channel). This value ranges from 0 to 10 seconds. The no form of the command resets the LACP waittime to its default value. lacp wait-time <0-10> no lacp wait-time	Mode: Interface Config Mode (Physical Interface Mode)	1	**lacp wait-time 5**	Gi0/8 is configured for LACP. Gi0/8 is selected. LACP Wait-time: 2. Enter the command. Using the command **show interfaces etherchannel** you can check if LACP Wait-time is set to 5.	LACP Wait-time: 5.
		2	**no lacp wait-time**	Gi0/8 is configured for LACP. Gi0/8 is selected. LACP Wait-time: 5. Enter the command. Using the command **show interfaces etherchannel** you can check if LACP Wait-time is set to 2.	LACP Wait-time: 2.

14.10 LACP Timeout

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link. The no form of the command sets the LACP timeout period to its default value. acp timeout { long | short } no lacp timeout	Mode: Interface Config Mode (Physical Interface Mode)	1	**lacp timeout short**	Gi0/8 is configured for LACP. Gi0/8 is selected. LACP Timeout: Long. Enter the command. Using the command **show interfaces etherchannel** you can check if LACP Timeout is set to Short.	LACP Timeout: Short.
		2	**lacp timeout long**	Gi0/8 is configured for LACP. Gi0/8 is selected. LACP Timeout: Short. Enter the command. Using the command **show interfaces etherchannel** you can check if LACP Timeout is set to Long.	LACP Timeout: Long.
		3	**no lacp timeout**	Gi0/8 is configured for LACP. Gi0/8 is selected. LACP Timeout: Short. Enter the command. Using the command **show interfaces etherchannel** you can check if LACP Timeout is set to default value Long.	LACP Timeout: Long.

14.11 LACP Rate

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the LACP rate. This command is a standardized implementation of the existing command; lacp timeout. It operates similar to the existing command. The no form of the command sets the LACP rate to its default value. lacp rate {normal | fast } no lacp rate	Mode: Interface Config Mode (Physical Interface Mode)	1	**lacp rate fast**	Gi0/8 is configured for LACP. Gi0/8 is selected. LACP Timeout: Long. Enter the command. Using the command **show interfaces etherchannel** you can check if LACP Timeout is set to Short.	LACP Timeout: Short.
		2	**lacp rate normal**	Gi0/8 is configured for LACP. Gi0/8 is selected. LACP Timeout: Short. Enter the command. Using the command **show interfaces etherchannel** you can check if LACP Timeout is set to Long.	LACP Timeout: Long.
		3	**no lacp rate**	Gi0/8 is configured for LACP. Gi0/8 is selected. LACP Timeout: Short. Enter the command. Using the command **show interfaces etherchannel** you can check if LACP Timeout is set to default value Long.	LACP Timeout: Long.

14.12 LACP Admin-Key

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the LACP actor admin key and LACP mode for a port. lacp admin-key <(Admin Key)1-65535> [mode { active | passive }]	Mode: Interface Config Mode (Physical Interface Mode)	1	**lacp admin-key 1 mode active**	Port Gi0/7 is default port for the Port Channel with ID 1. Gi0/7 is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/7 etherchannel** you can check if LACP actor admin key is configured and LACP Activity is set to Active.	LACP actor admin key is configured and LACP Activity is set to Active.
		2	**lacp admin-key 1 mode passive**	Port Gi0/7 is default port for the Port Channel with ID 1. Gi0/7 is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/7 etherchannel** you can check if LACP actor admin key is configured and LACP Activity is set to Passive.	LACP actor admin key is configured and LACP Activity is set to Passive.

14.13 fault Port

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the port that should be set as default port for a port channel. The configured port attaches with the port channel and participates only in dynamic aggregation selection. The no form of the command deletes the default port assigned for the port channel. default port <interface-type> <interface-id> no default port	Mode: Interface Config Mode (Port Channel Interface Mode)	1	**default port gigabitethernet 0/7**	LA is started and enabled. Port Channel with ID 1 is enabled. Port Channel with ID 1 is selected. Enter the command. Using the command **show interfaces gigabitethernet 0/7 etherchannel** you can check if port Gi0/7 is set as default port for a Port Channel with ID 1.	Gi0/7 is set as default port for a Port Channel with ID 1.
		2	**no default port**	LA is started and enabled. Port Channel with ID 1 is enabled. Port Channel with ID 1 is selected. Gi0/7 is set as default port for a Port Channel with ID 1. Enter the command. Using the command **show interfaces gigabitethernet 0/7 etherchannel** you can check if default port Gi0/7 assigned for the Port Channel is deleted.	Default port Gi0/7 assigned for the Port Channel is deleted.

14.14 Port-Channel Max-Ports

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the maximum number of ports that can be attached to a port channel. This value ranges between 2 and 8. The best ports are maintained in active state and other ports are maintained in standby state, if the total number of ports attached to the port -channel exceeds the configured value. port-channel max-ports <integer (2-8)>	Mode: Interface Config Mode (Port Channel Interface Mode)	1	**port-channel max-ports 2**	Maximum number of Ports is 8. Enter the command. Using the command **show interfaces etherchannel** you can check if Maximum number of Ports is set to 2.	Maximum number of Ports is 2.

14.15 Show Etherchannel

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays Etherchannel information for all port -channel groups created in the switch. This information contains admin and oper status of port -channel module, and status of protocol operate mode for each group. show etherchannel [[channel-group-number] { detail | load-balance | port | port-channel | summary | protocol }]	Mode: Privileged EXEC Mode	1	**show etherchannel**	Enter the command. You can check if Etherchannel information (admin and oper status of port -channel module, and status of protocol operate mode for each group) for all Port Channel groups created in the switch is displayed.	Etherchannel information (admin and oper status of port -channel module, and status of protocol operate mode for each group) for all Port Channel groups created in the switch is displayed.
		2	**show etherchannel detail**	Enter the command. You can check if detailed Etherchannel information is displayed.	Detailed Etherchannel information is displayed.
		3	**show etherchannel load-balance**	Enter the command. You can check if the load balancing policy applied for each Port Channel groups is displayed.	The load balancing policy applied for each Port Channel groups is displayed.
		4	**show etherchannel port**	Enter the command. You can check if the status of protocol operate mode and port details (port state, group to which the port belongs, port mode, aggregation state, Port Channel ID, pseudo Port Channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout) for each group are displayed.	The status of protocol operate mode and port details (port state, group to which the port belongs, port mode, aggregation state, Port Channel ID, pseudo Port Channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout) for each group are displayed.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**show etherchannel port-channel**	Enter the command. You can check if the admin and oper status of Port Channel module, and Port Channel details (Port Channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate mode, aggregator MAC and default port ID) are displayed.	The admin and oper status of Port Channel module, and Port Channel details (Port Channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate mode, aggregator MAC and default port ID) are displayed.
		6	**show etherchannel protocol**	Enter the command. You can check if the status of protocol operate mode for each Port Channel group is displayed.	The status of protocol operate mode for each Port Channel group is displayed.
		7	**show etherchannel summary**	Enter the command. You can check if the admin and oper status of Port Channel module, number of channel groups used, number of aggregators, group IDs, and Port Channel ID, status of protocol operate mode and member ports for each group are displayed.	The admin and oper status of Port Channel module, number of channel groups used, number of aggregators, group IDs, and Port Channel ID, status of protocol operate mode and member ports for each group are displayed.

14.16 Show Interfaces

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays Etherchannel details for all aggregated ports and port channels. The port details contain port state, group to which the port belongs, port mode, aggregation state, port channel ID, pseudo port channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate mode, aggregator MAC and default port ID. show interfaces [<interface-type> <interface-id>] etherchannel	Mode: Privileged EXEC Mode	1	**show interfaces gigabitethernet 0/1 etherchannel**	Enter the command. You can check if Etherchannel details (port details: port state, group to which the port belongs, port mode, aggregation state, Port Channel ID, pseudo Port Channel ID, admin key, oper key, port number, port state, and LACP port -priority, wait-time, port identifier, activity and timeout) for the specified type of interface (Gi0/1) are displayed.	Etherchannel details for the specified type of interface (Gi0/1) are displayed.
		2	**show interfaces etherchannel**	Enter the command. You can check if Etherchannel details (port details: port state, group to which the port belongs, port mode, aggregation state, Port Channel ID, pseudo Port Channel ID, admin key, oper key, port number, port state, and LACP port -priority, wait-time, port identifier, activity and timeout; Port Channel details: Port Channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate mode, aggregator MAC and default port ID) for all aggregated ports and Port Channels are displayed.	Etherchannel details for all aggregated ports and Port Channels are displayed.

14.17 Show LACP

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays LACP counter/neighbor information for all port channels. show lacp [<port-channel(1-65535)>] { counters | neighbor [detail] }	Mode: Privileged EXEC Mode	1	**show lacp counters**	Enter the command. You can check if LACP counter information (port ID, LACPDUs sent and received, number of markers sent and received, number of marker response sent and received, number of LACPDUs packets and number of LACPDUs errors) is displayed.	LACP counter information is displayed.
		2	**show lacp 234 counters**	Enter the command. You can check if LACP counter information (port ID, LACPDUs sent and received, number of markers sent and received, number of marker response sent and received, number of LACPDUs packets and number of LACPDUs errors) for the specified Port Channel 234 is displayed.	LACP counter information for the specified Port Channel 234 is displayed.
		3	**show lacp neighbor**	Enter the command. You can check if LACP neighbor information (partner system ID, flags details, LACP partner port priority, operational key, and port state) is displayed.	LACP neighbor information is displayed.
		4	**show lacp neighbor detail**	Enter the command. You can check if detailed LACP neighbor information (partner system ID, flags, aggregation state, and LACP partner port priority, partner oper key, partner port state, activity and timeout) is displayed.	Detailed LACP neighbor information is displayed.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**show lacp 234 neighbor**	Enter the command. You can check if neighbor information (partner system ID, flags details, LACP partner port priority, operational key, and port state) for the specified Port Channel 234 is displayed.	Neighbor information for the specified Port Channel 234 is displayed.
		6	**show lacp 234 neighbor detail**	Enter the command. You can check if detailed LACP neighbor information (partner system ID, flags, aggregation state, and LACP partner port priority, partner oper key, partner port state, activity and timeout) for the specified Port Channel 234 is displayed.	Detailed LACP neighbor information for the specified Port Channel 234 is displayed.

15. IGMP

15.1 IP IGMP Snooping

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables IGMP snooping in the switch/ a specific VLAN. If Enabled in a switch or interface, it learns the host's intention to listen to a specific multicast address. If Receiving any packets from the specified multicast address, the switch forwards these packets to the host listening to that address. Broadcasting is avoided to save bandwidth. If IGMP snooping is enabled globally, it is enabled in all existing VLAN interfaces. The no form of the command disables IGMP snooping in the switch/a specific VLAN. If IGMP snooping is disabled globally, it is disabled in all existing VLAN interfaces. ip igmp snooping [vlan <vlanid/ vfi_id>] no ip igmp snooping [vlan <vlanid/vfi_id>]	Mode: Global Config Mode / Config-VLAN Mode	1	**ip igmp snooping**	GMRP is disabled. IGMP snooping is disabled in the switch. Enter the command. Using the command **show ip igmp snooping globals** you can check if IGMP snooping is enabled in the switch.	IGMP snooping is enabled in the switch.
		2	**no ip igmp snooping**	GMRP is disabled. IGMP snooping is enabled in the switch. Enter the command. Using the command **show ip igmp snooping globals** that IGMP snooping is disabled in the switch.	IGMP snooping is disabled in the switch.

Command Description	Pre-Conditions	#	Step	Description	Result
		3	**ip igmp snooping vlan 1**	GMRP is disabled. IGMP snooping is disabled in VLAN with ID 1. Enter the command. Using the command **show ip igmp snooping** you can check if IGMP snooping is enabled in VLAN with ID 1.	IGMP snooping is enabled in VLAN with ID 1.
		4	**no ip igmp snooping vlan 1**	GMRP is disabled. IGMP snooping is enabled in VLAN with ID 1. Enter the command. Using the command **show ip igmp snooping** you can check if IGMP snooping is disabled in VLAN with ID 1.	IGMP snooping is disabled in VLAN with ID 1.

15.2 IP IGMP Snooping Proxy-Reporting

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables proxy reporting in the IGMP snooping switch. If enabled, the switch supports the multicast router to learn the membership information of the multicast group. It forwards the multicast packets based on group membership information. The proxy-reporting switch acts as a querier to the downstream hosts. It sends proxy-reporting to upstream queriers. The no form of the command disables proxy reporting in the IGMP snooping switch. ip igmp snooping proxy-reporting no ip igmp snooping proxy-reporting	Mode: Global Config Mode	1	**ip igmp snooping proxy-reporting**	Proxy is disabled in the switch. Proxy Reporting is globally disabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Proxy Reporting is globally enabled.	Proxy Reporting is globally enabled.

Command Description	Pre-Conditions	#	Step	Description	Result
		2	**no ip igmp snooping proxy-reporting**	Proxy is disabled in the switch. Proxy Reporting is globally enabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Proxy Reporting is globally disabled.	Proxy Reporting is globally disabled.

15.3 Snooping Multicast-Forwarding-Mode

Command Description	Pre-Conditions	#	Step	Description	Result
This command specifies the snooping multicast forwarding mode (IP-based or MAC-based). If ip mode is selected, and PIM and IGS are enabled, the L3 bitmap in the IPMC table is updated by PIM. The corresponding L2 bitmap is updated by querying the IGS to obtain Portlist. If PIM is disabled, IGS updates the L2 bitmap in the IPMC table directly. If the mode is MAC-based, the L2 bitmap is updated by PIM which queries the VLAN to obtain Portlist. If PIM is disabled, the IGS updates the L2 bitmap directly. snooping multicast-forwarding-mode { ip | mac }	Mode: Global Config Mode	1	**snooping multicast-forwarding-mode ip**	Enter the command. Multicast forwarding mode is MAC-based. Using the command **show ip igmp snooping globals** you can check if Multicast forwarding mode is IP-based.	Multicast forwarding mode is IP-based.
		2	**snooping multicast-forwarding-mode mac**	Enter the command. Multicast forwarding mode is IP-based. Using the command **show ip igmp snooping globals** you can check if Multicast forwarding mode is MAC-based.	Multicast forwarding mode is MAC-based.

15.4 IP IGMP Snooping MRouter-Time-Out

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time-out timer for each learnt router port. The router sends control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds. The no form of the command sets the IGMP snooping router port purge time-out to default value. ip igmp snooping mrouter-time-out <(60 - 600) seconds> no ip igmp snooping mrouter-time-out	Mode: Global Config Mode	1	**ip igmp snooping mrouter-time-out 60**	Router port purge interval is 125. Enter the command. Using the command **show ip igmp snooping globals** you can check if Router port purge interval is set to 60.	Router port purge interval is 60.
		2	**no ip igmp snooping mrouter-time-out**	Router port purge interval is 60. Enter the command. Using the command **show ip igmp snooping globals** you can check if Router port purge interval is set to 125.	Router port purge interval is 125.

15.5 IP IGMP Querier-Timeout

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time-out timer for each learnt router port. The routers send control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds. This command is a standardized implementation of the existing command; ip igmp snooping mroutertime-out. It operates similar to the existing command. ip igmp querier-timeout <(60 - 600) seconds>	Mode: Global Config Mode	1	**ip igmp querier-timeout 60**	Router port purge interval is 125. Enter the command. Using the command **show ip igmp snooping globals** you can check if Router port purge interval is set to 60.	Router port purge interval is 60.

15.6 IP IGMP Snooping Port-Purge-Interval

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the IGMP snooping port purge time interval. Whenever the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds. The no form of the command sets the IGMP snooping port purge time to default value. ip igmp snooping port-purge-interval <(130 - 1225) seconds> no ip igmp snooping port-purge-interval	Mode: Global Config Mode	1	**ip igmp snooping port-purge-interval 130**	Port purge interval is 260. Enter the command. Using the command **show ip igmp snooping** you can check if Port purge interval is set to 130.	Port purge interval is 130.
		2	**no ip igmp snooping port-purge-interval**	Port purge interval is 130. Enter the command. Using the command **show ip igmp snooping** you can check if Port purge interval is set to default value 260.	Port purge interval is 260.

15.7 IGMP Snooping Source-Only-Learning Age-Timer

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the IGMP snooping port purge time interval. Whenever the port receives reports from hosts, the timer is initiated. If the port receives another report before the timer expires, the timer is restarted. If the port does not receive any report from hosts till the timer expires, then the port entry is purged from the multicast database. The purge time interval value ranges between 130 and 1225 seconds. This command is a standardized implementation of the existing command; ip igmp snooping port-purge-interval. It operates similar to the existing command. ip igmp snooping source-only learning age-timer <short(130-1225)> no ip igmp snooping source-only learning age-timer	Mode: Global Config Mode	1	**ip igmp snooping source-only learning age-timer 130**	Port purge interval is 260. Enter the command. Using the command **show ip igmp snooping** you can check if Port purge interval is set to 130.	Port purge interval is 130.
		2	**no ip igmp snooping source-only learning age-timer**	Port purge interval is 130. Enter the command. Using the command **show ip igmp snooping** you can check if Port purge interval is set to default value 260.	Port purge interval is 260.

15.8 IP IGMP Snooping Report-Suppression-Interval

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the IGMP snooping report-suppression-interval time. The switch forwards IGMPv2 report message to the multicast group. A timer is started immediately after forwarding the report message and runs for set period of time. During this interval the switch does not forward another IGMPv2 report message addressed to the same multicast group to the router ports. The no form of the command sets the IGMP snooping report-suppression-interval time to the default value. ip igmp snooping report-suppression-interval <(1 - 25) seconds> no ip igmp snooping report-suppression-interval	Mode: Global Config Mode	1	**ip igmp snooping report-suppression-interval 17**	Report forward interval is 5. Enter the command. Using the command **show ip igmp snooping globals** you can check if Report forward interval is set to 17.	Report forward interval is 17.
		2	**no ip igmp snooping report-suppression-interval**	Report forward interval is 17. Enter the command. Using the command **show ip igmp snooping globals** you can check if Report forward interval is set to default value 5.	Report forward interval is 5.

15.9 IP IGMP Snooping Retry-Count

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the maximum number of group specific queries sent by the switch to check if there are any interested v2 receivers for the group after it received a leave message in the proxy/ proxyreporting mode. The port is deleted from the group membership information in the forwarding database if the maximum retry count exceeds set number. The no form of the command sets the number of group specific queries sent by the switch on reception of leave message to default value. ip igmp snooping retry-count <1 - 5> no ip igmp snooping retry-count	Mode: Global Config Mode	1	**ip igmp snooping retry-count 1**	Group specific query retry count is 2. Enter the command. Using the command **show ip igmp snooping globals** you can check if Group specific query retry count is set to 1.	Group specific query retry count is 1.
		2	**no ip igmp snooping retry-count**	Group specific query retry count is 1. Enter the command. Using the command **show ip igmp snooping globals** you can check if Group specific query retry count is set to default value 2.	Group specific query retry count is 2.

15.10 IP IGMP Snooping Group-Query-Interval

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group after it received a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database. The no form of the commands sets the group specific query interval time to default value. ip igmp snooping group-query-interval <(2-5) seconds> no ip igmp snooping group-query-interval	Mode: Global Config Mode	1	**ip igmp snooping group-query-interval 3**	Group specific query interval is 5. Enter the command. Using the command **show ip igmp snooping globals** you can check if Group specific query interval is set to 3.	Group specific query interval is 3.
		2	**no ip igmp snooping group-query-interval**	Group specific query interval is 3. Enter the command. Using the command **show ip igmp snooping globals** you can check if Group specific query interval is set to default value 2.	Group specific query interval is 2.

15.11 IP IGMP Snooping Report-Forwarding

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the IGMP reports to be forwarded to all ports, router ports of a VLAN or non-edge ports. The configuration enables the switch to forward IGMP report messages to the selected ports thus avoiding flooding of the network. The no form of the command sets IGMP report-forwarding status to default value. ip igmp snooping report-forward { all-ports | router-ports | non-edge-ports } no ip igmp snooping report-forward	Mode: Global Config Mode	1	**ip igmp snooping report-forward all-ports**	Reports are forwarded on router ports. Enter the command. Using the command **show ip igmp snooping globals** you can check if Reports are forwarded on all ports.	Reports are forwarded on all ports.
		2	**ip igmp snooping report-forward router-ports**	Reports are forwarded on all ports. Enter the command. Using the command **show ip igmp snooping globals** you can check if Reports are forwarded on router ports.	Reports are forwarded on router ports.
		3	**ip igmp snooping report-forward non-edge-ports**	Reports are forwarded on router ports. Enter the command. Using the command **show ip igmp snooping globals** you can check if Reports are forwarded on non-edge ports.	Reports are forwarded on non-edge ports.
		4	**no ip igmp snooping report-forward**	Reports are forwarded on non-edge ports. Enter the command. Using the command **show ip igmp snooping globals** you can check if Reports are forwarded on router ports.	Reports are forwarded on router ports.

15.12 IP IGMP Snooping Query-Forward

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the IGMP queries to be forwarded to all Vlan member ports or only to non-router ports. This configuration directs the queries to the selected ports to avoid flooding of the network. The queries are forwarded to multicast groups. If the Vlan module is enabled, IGMP snooping sends and receives the multicast packets through Vlan module. If Vlan is disabled, it sends the multicast packets through Bridge initialization/shutdown submodule. ip igmp snooping query-forward { all-ports | non-router-ports }	Mode: Global Config Mode	1	**ip igmp snooping query-forward all-ports**	Queries are forwarded on non-router ports. Enter the command. Using the command **show ip igmp snooping globals** you can check if Queries are forwarded on all ports.	Queries are forwarded on all ports.
		2	**ip igmp snooping query-forward non-router-ports**	Queries are forwarded on all ports. Enter the command. Using the command **show ip igmp snooping globals** you can check if Queries are forwarded on non-router ports.	Queries are forwarded on non-router ports.

15.13 IP IGMP Snooping Version

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the operating version of the IGMP snooping switch for a specific VLAN. The version can be set manually to execute condition specific commands. ip igmp snooping version { v1 | v2 | v3 }	Mode: Config-VLAN Mode	1	**ip igmp snooping version v1**	VLAN with ID=1 is selected. IGMP configured version is V3. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if IGMP configured version is set to V1.	IGMP configured version is V1.
		2	**ip igmp snooping version v2**	VLAN with ID=1 is selected. IGMP configured version is V1. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if IGMP configured version is set to V2.	IGMP configured version is V2.
		3	**ip igmp snooping version v3**	VLAN with ID=1 is selected. IGMP configured version is V2. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if IGMP configured version is set to V3.	IGMP configured version is V3.

15.14 IP IGMP Snooping Fast-Leave

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables fast leave processing and IGMP snooping for a specific VLAN, It enables IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled. If the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The no form of the command disables fast leave processing for a specific VLAN. ip igmp snooping fast-leave no ip igmp snooping fast-leave	Mode: Config-VLAN Mode	1	**ip igmp snooping fast-leave**	VLAN with ID=1 is selected. Fast leave is disabled. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Fast leave is enabled.	Fast leave is enabled.
		2	**no ip igmp snooping fast-leave**	VLAN with ID=1 is selected. Fast leave is enabled. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Fast leave is disabled.	Fast leave is disabled.

15.15 IP IGMP Snooping VLAN Immediate-Leave

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables fast leave processing and IGMP snooping for a specific VLAN, It enables IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled. If the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094. The no form of the command disables fast leave processing for a specific VLAN. This command is a standardized implementation of the existing command; ip igmp snooping fast-leave. It operates similar to the existing command. ip igmp snooping vlan <vlanid(1-4094)> immediate-leave no ip igmp snooping vlan <vlanid(1-4094)> immediate-leave	Mode: Global Config Mode	1	**ip igmp snooping vlan 1 immediate-leave**	Fast leave is disabled. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Fast leave is enabled.	Fast leave is enabled.
		2	**no ip igmp snooping vlan 1 immediate-leave**	Fast leave is enabled. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Fast leave is disabled.	Fast leave is disabled.

15.16 IP IGMP Snooping Querier

Command Description	Pre-Conditions	#	Step	Description	Result
This commands configures the IGMP snooping switch as a querier for a specific VLAN. Configured as a querier, the switch sends IGMP query messages. The query messages will be suppressed if there are any routers in the network. The no form of the command configures the IGMP snooping switch as non-querier for a specific VLAN. ip igmp snooping querier no ip igmp snooping querier	Mode: Config-VLAN Mode	1	**ip igmp snooping querier**	VLAN with ID=1 is selected. Snooping switch is configured as Non-Querier. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Snooping switch is configured as Querier.	Snooping switch is configured as Querier.
		2	**no ip igmp snooping querier**	VLAN with ID=1 is selected. Snooping switch is configured as Querier. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Snooping switch is configured as Non-Querier.	Snooping switch is configured as Non-Querier.

15.17 IP IGMP Snooping Querier-Interval

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the interval within which the general queries are sent by the IGMP snooping switch if configured as querier on a VLAN. The switch sends querier messages in proxy mode and proxyreporting mode to all downstream interfaces within this interval. The value range is between 60 to 600 seconds. The no form of the command sets the IGMP querier interval to default value. ip igmp snooping query-interval <(60 - 600) seconds> no ip igmp snooping query-interval	Mode: Config-VLAN Mode	1	**ip igmp snooping query-interval 60**	Query interval is 125. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Query interval is set to 60.	Query interval is 60.
		2	**no ip igmp snooping query-interval**	Query interval is 60. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Query interval is set to default value 125.	Query interval is 125.

15.18 IP IGMP Snooping Startup-Querier-Interval

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the time interval between the general query messages sent by the IGMP snooping switch, during startup of the querier election process. This time interval ranges between 15 and 150 seconds and should be less than or equal to query interval/4. The no form of the command sets the IGMP startup query interval to the default value. ip igmp snooping startup-query-interval <(15 - 150) seconds> no ip igmp snooping startup-query-interval	Mode: Config-VLAN Mode	1	**ip igmp snooping startup-query-interval 15**	Query Interval is 600. Startup Query Interval is 32. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Startup Query Interval is set to 15.	Startup Query Interval is 15.
		2	**no ip igmp snooping startup-query-interval**	Query Interval is 600. Startup Query Interval is 15. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Startup Query Interval is set to default value 32.	Startup Query Interval is 32.

15.19 IP IGMP Snooping Startup-Querier-Count

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the maximum number of general query messages sent out on switch startup, if the switch is configured as a querier. This value ranges between two and five. Startup query messages are sent to announce the presence of the switch along with its identity. The startup query count is manually configured to change the existing count. The no form of the command sets the number of general query messages sent out on switch startup, if the switch is configured as a querier to default value. ip igmp snooping startup-query-count <2 - 5> no ip igmp snooping startup-query-count	Mode: Config-VLAN Mode	1	**ip igmp snooping startup-query-count 3**	Startup Query Count is 5. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Startup Query Count is set to 3.	Startup Query Count is 3.
		2	**no ip igmp snooping startup-query-count**	Startup Query Count is 3. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Startup Query Count is set to default value 2.	Startup Query Count is 2.

15.20 IP IGMP Snooping Other-Querier-Present-Interval

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the maximum time interval to decide that another querier is present in the network. This time interval ranges between 120 and 1215 seconds. Within this time interval if the querier receives response from another querier, then the one with a higher IP address is announced as the querier for the network. The other querier present interval must be greater than or equal to ((Robustness Variable * Query Interval) + (Query Response Interval/2)). Here, Robustness value is 2. The no form of the command resets this interval to default value. ip igmp snooping other-querier-present-interval <value (120-1215) seconds> no ip igmp snooping other-querier-present-interval	Mode: Config-VLAN Mode	1	**ip igmp snooping other-querier-present-interval 120**	Other Querier Present Interval is 255. Robustness value is 2. Query Interval is 60. Query Response Interval is 0. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Other Querier Present Interval is set to 120.	Other Querier Present Interval is 120.
		2	**no ip igmp snooping other-querier-present-interval**	Other Querier Present Interval is 120. Robustness value is 2. Query Interval is 60. Query Response Interval is 0. Enter the command. Using the command **show ip igmp snooping vlan 1** you can check if Other Querier Present Interval is set to default value 255.	Other Querier Present Interval is 255.

15.21 IP IGMP Snooping MRouter

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, if IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled. Any IGMP message received on a switch is forwarded only on the router-ports and not on the host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network. The no form of the command deletes the statically configured router ports for a VLAN. ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...> no ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>	Mode: Config-VLAN Mode	1	**ip igmp snooping mrouter gigabitethernet 0/1-3**	VLAN 1 is selected. IGMP snooping is enabled. No list of multicast router ports is configured for the VLAN 1. Enter the command. Using the command **show ip igmp snooping mrouter** you can check if the list of multicast router ports (Gi0/1-3) for the VLAN 1 is configured.	The list of multicast router ports (Gi0/1-3) for the VLAN 1 is configured.
		2	**no ip igmp snooping mrouter gigabitethernet 0/2**	VLAN 1 is selected. IGMP snooping is enabled. The list of multicast router ports (Gi0/1-3) for the VLAN 1 is configured. Enter the command. Using the command **show ip igmp snooping mrouter** you can check if the statically configured router port Gi0/2 is deleted for the VLAN 1.	The statically configured router port Gi0/2 is deleted for the VLAN 1.

15.22 IP IGMP Snooping VLAN MRouter

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, if IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled. Any IGMP message received on a switch is forwarded only on the router-ports and not on host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network. The no form of the command deletes the statically configured router ports for a VLAN. This command is a standardized implementation of the existing command; ip igmp snooping mrouter. It operates similar to the existing command. ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...> no ip igmp snooping vlan <vlanid (1-4094)> mrouter <ifXtype> <0/a-b, 0/c, ...>	Mode: Global Config Mode	1	**ip igmp snooping vlan 1 mrouter gigabitethernet 0/1-3**	IGMP snooping is enabled. No list of multicast router ports is configured for the VLAN 1. Enter the command. Using the command **show ip igmp snooping mrouter** you can check if the list of multicast router ports (Gi0/1-3) for the VLAN 1 is configured.	The list of multicast router ports (Gi0/1-3) for the VLAN 1 is configured.
		2	**no ip igmp snooping vlan 1 mrouter gigabitethernet 0/2**	IGMP snooping is enabled. The list of multicast router ports (Gi0/1-3) for the VLAN 1 is configured. Enter the command. Using the command **show ip igmp snooping mrouter** you can check if the statically configured router port Gi0/2 is deleted for the VLAN 1.	The statically configured router port Gi0/2 is deleted for the VLAN 1.

15.23 Snooping Leave-Process Config-Level

Command Description	Pre-Conditions	#	Step	Description	Result
This command specifies the level of configuring the leave processing mechanisms. If the switch intercepts a leave group message on a switch port, it normally sends a query to that multicast group through the same switch port. If no hosts respond to the query and no multicast routers have been discovered on the switch port, that port is removed from the multicast group. snooping leave-process config-level { vlan | port }	Mode: Global Config Mode	1	**snooping leave-process config-level vlan**	Leave config level is Port-based. Enter the command. Using the command **show ip igmp snooping globals** you can check if Leave config level is VLAN-based.	Leave config level is VLAN-based.
		2	**snooping leave-process config-level port**	Leave config level is Vlan-based. Enter the command. Using the command **show ip igmp snooping globals** you can check if Leave config level is Port-based.	Leave config level is Port-based.

15.24 IP IGMP Snooping Enhanced-Mode

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures snooping system enhanced mode in the switch. It is a mode of operation provided to enhance the operation of IGMP snooping module to duplicate Multicast traffic by learning Multicast group entries based on the Port and Inner Vlan. This mode of operation is applied if the down stream devices are less intelligent or not capable of duplicating Multicast traffic. ip igmp snooping enhanced-mode { enable | disable }	Mode: Global Config Mode	1	**ip igmp snooping enhanced-mode enable**	Snooping mode is set as IP-based. IGMP Snooping Enhanced mode is disabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if IGMP Snooping Enhanced mode is enabled.	IGMP Snooping Enhanced mode is enabled.
		2	**ip igmp snooping enhanced-mode disable**	Snooping mode is set as IP-based. IGMP Snooping Enhanced mode is enabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if IGMP Snooping Enhanced mode is disabled.	IGMP Snooping Enhanced mode is disabled.

15.25 IP IGMP Snooping Sparse-Mode

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures snooping system sparse mode in the switch. In the sparse mode, the IGS module drops the unknown multicast traffic if there is no listener for the multicast data. In the non-sparse-mode, the IGS module forwards the unknown multicast traffic. The multicast data gets flooded to the member port of vlan. ip igmp snooping sparse-mode { enable | disable }	Mode: Global Config Mode	1	**ip igmp snooping sparse-mode enable**	Snooping mode is set as MAC-based. IGMP Snooping Sparse mode is disabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if IGMP Snooping Sparse mode is enabled.	IGMP Snooping Sparse mode is enabled.
		2	**ip igmp snooping sparse-mode disable**	Snooping mode is set as MAC-based. IGMP Snooping Sparse mode is enabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if IGMP Snooping Sparse mode is disabled.	IGMP Snooping Sparse mode is disabled.

15.26 Snooping Report-Process Config-Level

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the configuration-level for report processing as non-router ports or as all ports. snooping report-process config-level { non-router-ports | all-ports }	Mode: Global Config Mode	1	**snooping report-process config-level non-router-ports**	Report processing config level is on all-ports. Enter the command. Using the command **show ip igmp snooping globals** you can check if Report processing config level is on non-router-ports.	Report processing config level is on non-router-ports.
		2	**snooping report-process config-level all-ports**	Report processing config level is on non-router-ports. Enter the command. Using the command **show ip igmp snooping globals** you can check if Report processing config level is on all-ports.	Report processing config level is on all-ports.

15.27 Multicast VLAN Routing (MVR)

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the multicast VLAN feature on a port. Multicast VLAN feature is used for applications where wide-scale deployment of multicast traffic is necessary. MVLAN Registration allows a subscriber on a port to subscribe and unsubscribe to a particular multicast stream on any of the multicast VLANs. Multicast VLANs enable efficient multicast data flow in separate M-VLANs, while normal data flows through VLANs. The no form of this command disables the multicast VLAN feature. This command is a standardized implementation of the existing command; ip igmp snooping multicastvlan. It operates similar to the existing command. mvr no mvr	Mode: Global Config Mode	1	**mvr**	Multicast VLAN is disabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Multicast VLAN is enabled.	Multicast VLAN is enabled.
		2	**no mvr**	Multicast VLAN is enabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Multicast VLAN is disabled.	Multicast VLAN is disabled.

15.28 IP IGMP Snooping Filter

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the IGMP snooping filter. The IGS filtering feature restricts channel registration from being added to the database. In transparent snooping, the filtered packet will not be added to the snooping database but will be forwarded upstream. If disabled, all the filter related configurations remain but the incoming reports will not be subject to filtering. IGS module programs the hardware to remove the configured rate limit. It flushes all the registrations learnt through a port if a threshold limit is configured for this interface. The no form of the command disables the IGMP snooping filter. ip igmp snooping filter no ip igmp snooping filter	Mode: Global Config Mode	1	**ip igmp snooping filter**	Snooping filter is disabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Snooping filter is enabled.	Snooping filter is enabled.
		2	**no ip igmp snooping filter**	Snooping filter is enabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Snooping filter is disabled.	Snooping filter is disabled.

15.29 IP IGMP Snooping Blocked-Router

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures a static router port as blocked router port. If configured as a blocked router, the queries, PIM DVMRP and data messages are discarded. The corresponding port entry is removed from the forwarding database. The ports to be configured as blocked router ports must not be configured as static router ports. The no form of the command resets the blocked router ports to normal router port. ip igmp snooping blocked-router <interface-type> <0/a-b, 0/c, ...> no ip igmp snooping blocked-router <interface-type> <0/a-b, 0/c, ...>	Mode: Config-VLAN Mode	1	**ip igmp snooping blocked-router gigabitethernet 0/3-5**	No ports are set as blocked. No ports are set as static. Enter the command. Using the command **show ip igmp snooping blocked-router** you can check if the list of router ports (Gi0/3-5) to be set as blocked is configured.	Router ports Gi0/3-5 are set as blocked.
		2	**no ip igmp snooping blocked-router gigabitethernet 0/3**	Router ports (Gi0/3-5) are set as blocked. No ports are set as static. Enter the command. Using the command **show ip igmp snooping blocked-router** you can check if the blocked router port Gi0/3 is resetted to normal router port.	The blocked router port Gi0/3 is resetted to normal router port.

15.30 IP IGMP Snooping Leavemode

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the port leave mode for an interface. The mechanism to process the leave messages in the downstream is selected. The switch sends an IGMP query message to find if there are any host interested in the multicast group. ip igmp snooping leavemode { exp-hosttrack | fastLeave | normalleave } [InnerVlanId <short (1-4094)>]	Mode: Interface Config Mode	1	**ip igmp snooping leavemode exp-hosttrack InnerVlanId 1**	Gi0/1 is selected. Leave Process mode is Normal Leave. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Leave Process mode is set to Explicit Host Track.	Leave Process mode is Explicit Host Track.
		2	**ip igmp snooping leavemode fastLeave InnerVlanId 1**	Gi0/1 is selected. Leave Process mode is Explicit Host Track. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Leave Process mode is set to Fast Leave.	Leave Process mode is Fast Leave.
		3	**ip igmp snooping leavemode normalleave InnerVlanId 1**	Gi0/1 is selected. Leave Process mode is Fast Leave. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Leave Process mode is set to Normal Leave.	Leave Process mode is Normal Leave.

15.31 IP IGMP Snooping Ratelimit

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the rate limit for a downstream interface in units of the number of IGMP packets per second. The switch allows to configure the maximum rate of IGMP reports incoming for a port. The IGMP rate limiting eliminates the bursts or attacks from specific physical port. It prevents the exhaustion of system resources. The no form of the command resets the rate limit to default value for an interface. By default, the rate limit will hold the maximum value supported by an unsigned integer and will not rate limit any IGMP packets. ip igmp snooping ratelimit <integer> [InnerVlanId <short (1-4094)>] no ip igmp snooping ratelimit [InnerVlanId <short (1-4094)>]	Mode: Interface Config Mode	1	**ip igmp snooping ratelimit 0 InnerVlanId 1**	Gi0/1 is selected. Rate Limit on the interface is 4294967295. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Rate Limit on the interface is set to 0.	Rate Limit on the interface is 0.
		2	**no ip igmp snooping ratelimit InnerVlanId 1**	Gi0/1 is selected. Rate Limit on the interface is 0. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Rate Limit on the interface is set to default value 4294967295.	Rate Limit on the interface is 4294967295.

15.32 IP IGMP Snooping Limit

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the maximum limit type for an interface. The maximum limit is the number of unique registrations for a channel or group. The no form of the command configures the maximum limit type as none for an interface. ip igmp snooping limit { channels | groups } <interger32> [InnerVlanId <short (1-4094)>] no ip igmp snooping limit [InnerVlanId <short (1-4094)>]	Mode: Interface Config Mode	1	**ip igmp snooping limit channels 20 InnerVlanId 1**	Gi0/1 is selected. Max Limit Type is None. Max limit is 0. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Max Limit Type is set to Channels and Max limit is 20.	Max Limit Type is Channels. Max limit is 20.
		3	**no ip igmp snooping limit InnerVlanId 1**	Gi0/1 is selected. Max Limit Type is Groups. Max limit is 20. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Max Limit Type is set to None and Max limit is 0.	Max Limit Type is None. Max limit is 0.

15.33 IP IGMP Snooping Filter-ProfileID

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the multicast profile index for a downstream interface. This profile contains a set of allowed or denied rules to be applied for the IGMP packets received through this downstream interface. The no form of the command resets the multicast profile index to default value. ip igmp snooping filter-profileId <integer> [InnerVlanId <short (1-4094)>] no ip igmp snooping filter-profileId [InnerVlanId <short (1-4094)>]	Mode: Interface Config Mode	1	**ip igmp snooping filter-profileId 20 InnerVlanId 1**	Gi0/1 is selected. Profile ID is 0. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Profile ID is set to 20.	Profile ID is 20.
		2	**no ip igmp snooping filter-profileId InnerVlanId 1**	Gi0/1 is selected. Profile ID is 20. Enter the command. Using the command **show ip igmp snooping port-cfg** you can check if Profile ID is set to default value 0.	Profile ID is 0.

15.34 IP IGMP Snooping Proxy

Command Description	Pre-Conditions	#	Step	Description	Result
This command enables proxy in the IGMP snooping switch. In proxy mode, the switch acts as a querier for all downstream interfaces and a host for all upstream interfaces. The switch sends general query to all downstream interfaces at the query interval and collects information about the member ports. The proxy sends current consolidated report and state change report to upstream interfaces. The no form of the command disables proxy in the IGMP snooping switch. ip igmp snooping proxy no ip igmp snooping proxy	Mode: Global Config Mode	1	**ip igmp snooping proxy**	Proxy-reporting globally disabled. Proxy globally disabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Proxy globally enabled.	Proxy globally enabled.
		2	**no ip igmp snooping proxy**	Proxy-reporting globally disabled. Proxy globally enabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Proxy globally disabled.	Proxy globally disabled.

15.35 IP IGMP Snooping Max-Response-Code

Command Description	Pre-Conditions	#	Step	Description	Result
This command sets the maximum response code inserted in general queries sent to host. The unit of the response code is a tenth a second. The value ranges between 0 and 255. The no form of the command sets the query response code to default value. ip igmp snooping max-response-code <(0 - 255)> no ip igmp snooping max-response-code	Mode: Config-VLAN Mode	1	**ip igmp snooping max-response-code 10**	Max Response Code is 100. Enter the command. Using the command **show ip igmp snooping** you can check if Max Response Code is set to 10.	Max Response Code is 10.
		2	**no ip igmp snooping max-response-code**	Max Response Code is 10. Enter the command. Using the command **show ip igmp snooping** you can check if Max Response Code is set to default value 100.	Max Response Code is 100.

15.36 IP IGMP Snooping MRouter-Port Purge Time-Out

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the router port purge time-out interval for a VLAN. The time interval after which the proxy assumes there are no v1/v2 routers present on the upstream port. While the older querier timer is running, the proxy replies to all the queries with consolidated v1/v2 reports. If the timer expires and the v2/v3 queriers are not present the dynamically learnt port is purged. If the port is static, router port, the proxy replies to all queries with a new version of v2/v3 consolidated reports. The no form of the command resets the router port purge time-out interval to default, for a VLAN. ip igmp snooping mrouter-port <ifXtype> <iface_list> time-out <short(60-600)> no ip igmp snooping mrouter-port <interface-type> <0/a-b, 0/c, ...>	Mode: Config-VLAN Mode	1	**ip igmp snooping mrouter-port gigabitethernet 0/1 time-out 60**	The router ports are statically configured for the VLAN 1. Router port purge time-out interval is 125. Enter the command. Using the command **show ip igmp snooping mrouter detail** you can check if router port purge time-out interval is set to 60.	Router port purge time-out interval is 60.
		2	**no ip igmp snooping mrouter-port gigabitethernet 0/1 time-out**	The router ports are statically configured for the VLAN 1. Router port purge time-out interval is 60. Enter the command. Using the command **show ip igmp snooping mrouter detail** you can check if router port purge time-out interval is set to 125.	Router port purge time-out interval is 125.

15.37 IP IGMP Snooping MRouter-Port Version

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the operating version of IGMP PROXY on the upstream router port for a VLAN. The no form of the command resets the operating version of the IGMP PROXY on the upstream router port to its default operating version. ip igmp snooping mrouter-port <ifXtype> <iface_list> version { v1 | v2 | v3 } no ip igmp snooping mrouter-port <ifXtype> <iface_list> version	Mode: Config-VLAN Mode	1	**ip igmp snooping mrouter-port gigabitethernet 0/1 version v1**	IGMP Snooping version is v3. Enter the command. Using the command **show ip igmp snooping mrouter detail** you can check if IGMP Snooping version is set to v1.	IGMP Snooping version is v1.
		2	**ip igmp snooping mrouter-port gigabitethernet 0/1 version v2**	IGMP Snooping version is v1. Enter the command. Using the command **show ip igmp snooping mrouter detail** you can check if IGMP Snooping version is set to v2.	IGMP Snooping version is v2.
		3	**ip igmp snooping mrouter-port gigabitethernet 0/1 version v3**	IGMP Snooping version is v2. Enter the command. Using the command **show ip igmp snooping mrouter detail** you can check if IGMP Snooping version is set to v3.	IGMP Snooping version is v3.
		4	**no ip igmp snooping mrouter-port gigabitethernet 0/1 version**	IGMP Snooping version is v2. Enter the command. Using the command **show ip igmp snooping mrouter detail** you can check if IGMP Snooping version is set to default value v3.	IGMP Snooping version is v3.

15.38 Show IP IGMP Snooping MRouter

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified). The interface details and the corresponding port number along with its type (static/ dynamic are displayed. show ip igmp snooping mrouter [Vlan <vlan index>] [detail] [switch <switch_name>]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping mrouter**	Enter the command. You can check if the router ports for all VLANs are displayed.	Router ports for all VLANs are displayed.
		2	**show ip igmp snooping mrouter detail**	Enter the command. You can check if detailed information about the router ports for all VLANs is displayed.	Detailed information about the router ports for all VLANs is displayed.
		3	**show ip igmp snooping mrouter vlan 1**	Enter the command. You can check if the router ports for the VLAN 1 are displayed.	Router ports for the VLAN 1 are displayed.
		4	**show ip igmp snooping mrouter vlan 1 detail**	Enter the command. You can check if detailed information about the router ports for the VLAN 1 is displayed.	Detailed information about the router ports for the VLAN 1 is displayed.

15.39 Show IP IGMP Snooping Globals

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if switch is not specified). show ip igmp snooping globals [switch <switch_name>]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping globals**	Enter the command. You can check if IGMP snooping information for all VLANs is displayed.	IGMP snooping information for all VLANs is displayed.

15.40 Show IP IGMP Snooping

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all context (if no switch is specified). show ip igmp snooping [Vlan <vlan id>] [switch <switch_ name>]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping**	Enter the command. You can check if IGMP snooping information for all VLANs is displayed.	IGMP snooping information for all VLANs is displayed.
		2	**show ip igmp snooping vlan 1**	Enter the command. You can check if IGMP snooping information for the VLAN 1 is displayed.	IGMP snooping information for the VLAN 1 is displayed.

15.41 Show IP IGMP Snooping Groups

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays IGMP group information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switch (if no switch is specified) . It also displays the information for static / dynamic or both type of multicast entries. show ip igmp snooping groups [Vlan <vlan id> [Group <Address>]] [{ static | dynamic }] [switch <switch_name>]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping groups**	Enter the command. You can check if IGMP group information for all VLANs is displayed.	IGMP group information for all VLANs is displayed.
		2	**show ip igmp snooping groups static**	Enter the command. You can check if static multicast entries for all VLANs are displayed.	Only static multicast entries for all VLANs are displayed.
		3	**show ip igmp snooping groups dynamic**	Enter the command. You can check if dynamic multicast entries for all VLANs are displayed.	Only dynamic multicast entries for all VLANs are displayed.
		4	**show ip igmp snooping groups vlan 1**	Enter the command. You can check if IGMP group information for the VLAN 1 is displayed.	IGMP group information for the VLAN 1 is displayed.

15.42 Show IP IGMP Snooping Forwarding-Database

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays multicast forwarding entries for all VLANs or a specific VLAN for a given switch or for all switches (if no switch is specified). It also displays the information for static / dynamic or both type of multicast entries. show ip igmp snooping forwarding-database [Vlan <vlan-id>] [{ static | dynamic }] [switch <switch_name>]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping forwarding-database**	Enter the command. You can check if multicast forwarding entries for all VLANs are displayed.	Multicast forwarding entries for all VLANs are displayed.
		2	**show ip igmp snooping forwarding-database static**	Enter the command. You can check if static multicast forwarding entries for all VLANs are displayed.	Static multicast forwarding entries for all VLANs are displayed.
		3	**show ip igmp snooping forwarding-database dynamic**	Enter the command. You can check if dynamic multicast forwarding entries for all VLANs are displayed.	Dynamic multicast forwarding entries for all VLANs are displayed.
		4	**show ip igmp snooping forwarding-database vlan 1**	Enter the command. You can check if multicast forwarding entries for the VLAN 1 are displayed.	Multicast forwarding entries for the VLAN 1 are displayed.
		5	**show ip igmp snooping forwarding-database vlan 1 static**	Enter the command. You can check if static multicast forwarding entries for the VLAN 1 are displayed.	Multicast forwarding entries for the VLAN 1 are displayed.
		6	**show ip igmp snooping forwarding-database vlan 1 dynamic**	Enter the command. You can check if dynamic multicast forwarding entries for the VLAN 1 are displayed.	Dynamic multicast forwarding entries for the VLAN 1 are displayed.

15.43 Show IP IGMP Snooping Statistics

Command Description	Pre-Conditions	#	Step	Description	Result
This command Displays IGMP snooping statistics for all VLANs or a specific VLAN for a given switch or for all switch (if no switch is specified). show ip igmp snooping statistics [Vlan <vlan-id>] [switch <switch_name>]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping statistics**	Enter the command. You can check if IGMP snooping statistics for all VLANs are displayed.	IGMP snooping statistics for all VLANs are displayed.
		2	**show ip igmp snooping statistics vlan 1**	Enter the command. You can check if IGMP snooping statistics for the VLAN 1 are displayed.	IGMP snooping statistics for the VLAN 1 are displayed.

15.44 Show IP IGMP Snooping Blocked-Router

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the blocked router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified). show ip igmp snooping blocked-router [Vlan <vlan index>] [switch <switch_ name>]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping blocked-router**	Enter the command. You can check if the blocked router ports for all VLANs are displayed.	The blocked router ports for all VLANs are displayed.
		2	**show ip igmp snooping blocked-router vlan 1**	Enter the command. You can check if the blocked router ports for the VLAN 1 are displayed.	The blocked router ports for the VLAN 1 are displayed.

15.45 Show IP IGMP Snooping Multicast-Receivers

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays IGMP multicast host information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switches (if no switch is specified). show ip igmp snooping multicast-receivers [Vlan <vlan-id> [Group <Address>]] [switch <switch_name>]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping multicast-receivers**	Enter the command. You can check if IGMP multicast host information for all VLANs is displayed.	IGMP multicast host information for all VLANs is displayed.
		2	**show ip igmp snooping multicast-receivers vlan 1**	Enter the command. You can check if IGMP multicast host information for the VLAN 1 is displayed.	IGMP multicast host information for the VLAN 1 is displayed.

15.46 Show IP IGMP Snooping Port-Cfg

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays IGS Port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch. show ip igmp snooping port-cfg [{ interface <interface-type> <interface-id> [InnerVlanId vlan-id(1-4094)] | switch <switch_name> }]	Mode: Privileged EXEC Mode	1	**show ip igmp snooping port-cfg**	Enter the command. You can check if IGS Port configuration information for all Inner VLANs is displayed.	IGS Port configuration information for all Inner VLANs is displayed.
		2	**show ip igmp snooping port-cfg interface gigabitethernet 0/1**	Enter the command. You can check if IGS Port configuration information for Port Gi0/1 and all Inner VLANs is displayed.	IGS Port configuration information for Port Gi0/1 and all Inner VLANs is displayed.
		3	**show ip igmp snooping port-cfg interface gigabitethernet 0/1 InnerVlanId 1**	Enter the command. You can check if IGS Port configuration information for Port Gi0/1 and Inner VLAN 1 is displayed.	IGS Port configuration information for Port Gi0/1 and Inner VLAN 1 is displayed.

15.47 IP IGMP Snooping Clear Counters

Command Description	Pre-Conditions	#	Step	Description	Result
This command clears the IGMP snooping statistics maintained for VLAN(s). ip igmp snooping clear counters [Vlan <vlan-id (1-4094)>]	Mode: Global Config Mode	1	**ip igmp snooping clear counters**	Enter the command. Using the command **show ip igmp snooping statistics** you can check if IGMP snooping statistics for all VLANs are cleared.	IGMP snooping statistics for all VLANs are cleared.
		2	**ip igmp snooping clear counters vlan 1**	Enter the command. Using the command **show ip igmp snooping statistics** you can check if IGMP snooping statistics for VLAN 1 are cleared.	IGMP snooping statistics for VLAN 1 are cleared.

15.48 IP IGMP Snooping Send-Query

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the IGMP general query transmission feature upon the topology change in the switch. ip igmp snooping send-query { enable | disable }	Mode: Global Config Mode	1	**ip igmp snooping send-query enable**	Transmit Query on Topology Change is globally disabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Transmit Query on Topology Change is globally enabled.	Transmit Query on Topology Change is globally enabled.
		2	**ip igmp snooping send-query disable**	Transmit Query on Topology Change is globally enabled. Enter the command. Using the command **show ip igmp snooping globals** you can check if Transmit Query on Topology Change is globally disabled.	Transmit Query on Topology Change is globally disabled.

15.49 IP IGMP Snooping Static-Group

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures IGMP snooping static multicast in the multicast switch This no form of the command removes the IGMP snooping static multicast in the multicast switch ip igmp snooping static-group <mcast_addr> ports <ifXtype> <iface_list> no ip igmp snooping static-group <mcast_addr>	Mode: Config-VLAN Mode	1	**ip igmp snooping static-group 225.3.2.2 ports gigabitethernet 0/2**	IGMP snooping static multicast (225.3.2.2) doesn't exist in the multicast switch. Enter the command. Using the command **show ip igmp snooping groups static** you can check if IGMP snooping static multicast 225.3.2.2 is added in the multicast switch.	IGMP snooping static multicast 225.3.2.2 is added in the multicast switch.
		2	**no ip igmp snooping static-group 225.3.2.2**	IGMP snooping static multicast (225.3.2.2) exists in the multicast switch. Enter the command. Using the command **show ip igmp snooping groups static** you can check if IGMP snooping static multicast 225.3.2.2 is removed in the multicast switch.	IGMP snooping static multicast 225.3.2.2 is removed in the multicast switch.

16. MAC-Address-Table

16.1 MAC-Address-Table Aging-Time

Command Description	Pre-Conditions	#	Step	Description	Result
This command configures the timeout period (in seconds) for aging out dynamically learned forwarding information entry and static entry in the MAC-address-table. That is, the entry is deleted once the aging timer expires. This timeout period value ranges from 10 to 1000000 seconds. You should provide high value for the aging time to record dynamic entries for a longer time, if traffic is not frequent. This reduces the possibility of flooding. The no form of the command resets the maximum age of an entry in the MAC-address-table to its default value. mac-address-table aging-time <10 - 100000 seconds> no mac-address-table aging-time	Mode: Global Config Mode	1	**mac-address-table aging-time 200**	Enter the command. Using the command **show mac-address-table aging-time** you can check if aging time is set to 200.	Aging time is 200.
		2	**no mac-address-table aging-time**	Enter the command. Using the command **show mac-address-table aging-time** you can check if aging time is set to default value 300.	Aging time is 300.

16.2 Show MAC-Address-Table

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays all static / dynamic unicast and multicast MAC entries created in the MAC address table. These entries contain VLAN ID, unicast / multicast MAC address, unicast backbone MAC address of peer backbone edge bridge, member ports, the type of entry (that is static, learnt and so on), and total number of entries displayed. show mac-address-table [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]	Mode: Privileged EXEC Mode	1	**show mac-address-table**	Enter the command. You can check if all static / dynamic unicast and multicast MAC entries created in the MAC-address-table are displayed.	All static / dynamic unicast and multicast MAC entries created in the MAC-address-table are displayed.
		2	**show mac-address-table vlan 1**	Enter the command. You can check if all static / dynamic unicast and multicast MAC entries created in the MAC-address-table for the VLAN ID=1 are displayed.	All static / dynamic unicast and multicast MAC entries created in the MAC-address-table for the VLAN ID=1 are displayed.
		3	**show mac-address-table address 00:11:fc:08:80:c0**	Enter the command. You can check that all static / dynamic unicast and multicast MAC entries created in the MAC-address-table for the MAC address 00:11:FC:08:80:C0 are displayed.	All static / dynamic unicast and multicast MAC entries created in the MAC-address-table for the MAC address 00:11:FC:08:80:C0 are displayed.
		4	**show mac-address-table interface gigabitethernet 0/8**	Enter the command. You can check if all static / dynamic unicast and multicast MAC entries for the gigabitethernet interface 0/8 are displayed.	All static / dynamic unicast and multicast MAC entries for the gigabitethernet interface 0/8 are displayed.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**show mac-address-table vlan 1 address 00:11:fc:08:80:c0 interface gigabitethernet 0/8**	Enter the command. You can check if all static / dynamic unicast and multicast MAC entries for VLAN ID=1, MAC address 00:11:FC:08:80:C0 and gigabitethernet interface 0/8 are displayed.	All static / dynamic unicast and multicast MAC entries for VLAN ID=1, MAC address 00:11:FC:08:80:C0 and gigabitethernet interface 0/8 are displayed.

16.3 Show MAC-Address-Table Dynamic Unicast

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays all dynamically learnt unicast entries from the MAC address table. These entries contain VLAN ID for which unicast MAC address entry is learnt, unicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed. show mac-address-table dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]	Mode: Privileged EXEC Mode	1	**show mac-address-table dynamic unicast**	Enter the command. You can check if all dynamically learnt unicast entries from the MAC address table are displayed.	All dynamically learnt unicast entries from the MAC address table are displayed.
		2	**show mac-address-table dynamic unicast vlan 1**	Enter the command. You can check if all dynamically learnt unicast entries from the MAC address table for the VLAN ID=1 are displayed.	All dynamically learnt unicast entries from the MAC address table for the VLAN ID=1 are displayed.

Command Description	Pre-Conditions	#	Step	Description	Result
		3	**show mac-address-table dynamic unicast address 00:11:fc:08:80:c0**	Enter the command. You can check if all dynamically learnt unicast entries from the MAC address table for the specified unicast MAC address 00:11:FC:08:80:C0 are displayed.	All dynamically learnt unicast entries from the MAC address table for the specified unicast MAC address 00:11:FC:08:80:C0 are displayed.
		4	**show mac-address-table dynamic unicast interface gigabitethernet 0/1**	Enter the command. You can check if all dynamically learnt unicast entries from the MAC address table for the specified interface gigabitethernet 0/1 are displayed.	All dynamically learnt unicast entries from the MAC address table for the specified interface gigabitethernet 0/1 are displayed.
		5	**show mac-address-table dynamic unicast vlan 1 address 00:11:fc:08:80:c0 interface gigabitethernet 0/1**	Enter the command. You can check if all dynamically learnt unicast entries from the MAC address table for the VLAN ID=1, unicast MAC address 00:11:FC:08:80:C0 and interface gigabitethernet 0/1 are displayed.	All dynamically learnt unicast entries from the MAC address table for the VLAN ID=1, unicast MAC address 00:11:FC:08:80:C0 and interface gigabitethernet 0/1 are displayed.

16.4 Show MAC-Address-Table Dynamic Multicast

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays all dynamically learnt multicast entries from the MAC address table. These entries contain VLAN ID for which multicast MAC address entry is learnt, multicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed. show mac-address-table dynamic multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]	Mode: Privileged EXEC Mode	1	**show mac-address-table dynamic multicast**	Enter the command. You can check if all dynamically learnt multicast entries from the MAC address table are displayed.	All dynamically learnt multicast entries from the MAC address table are displayed.
		2	**show mac-address-table dynamic multicast vlan 1**	Enter the command. You can check if all dynamically learnt multicast entries from the MAC address table for the VLAN ID=1 are displayed.	All dynamically learnt multicast entries from the MAC address table for the VLAN ID=1 are displayed.
		3	**show mac-address-table dynamic multicast address 01:11:22:33:44:55**	Enter the command. You can check if all dynamically learnt multicast entries from the MAC address table for the specified unicast MAC address 01:11:22:33:44:55 are displayed.	All dynamically learnt multicast entries from the MAC address table for the specified unicast MAC address 01:11:22:33:44:55 are displayed.
		4	**show mac-address-table dynamic multicast interface gigabitethernet 0/1**	Enter the command. You can check if all dynamically learnt multicast entries from the MAC address table for the specified interface gigabitethernet 0/1 are displayed.	All dynamically learnt multicast entries from the MAC address table for the specified interface gigabitethernet 0/1 are displayed.

Command Description	Pre-Conditions	#	Step	Description	Result
		5	**show mac-address-table dynamic multicast**	Enter the command. You can check if all dynamically learnt multicast entries from the MAC address table for the VLAN ID=1, unicast MAC address 01:11:22:33:44:55 and interface gigabitethernet 0/1 are displayed.	All dynamically learnt multicast entries from the MAC address table for the VLAN ID=1, unicast MAC address 01:11:22:33:44:55 and interface gigabitethernet 0/1 are displayed.

16.5 Show MAC-Address-Table Aging-Time

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the ageing time configured for the MAC address table. This time denotes the interval (in seconds) after which the dynamically learned forwarding information entry and static entry in the MAC address table are deleted. show mac-address-table aging-time [switch <context_name>]	Mode: Privileged EXEC Mode	1	**show mac-address-table aging-time**	Enter the command. You can check if the aging time configured for the MAC address table is displayed.	MAC address aging time is displayed.

17. TCP

17.1 Show TCP Statistics

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the tcp statistics information such as Max connections, Active opens, Passive opens and attempts fail. show tcp statistics	Mode: Privileged EXEC Mode	1	**show tcp statistics**	Enter the command. You can check if the tcp statistics information such as Max connections, Active opens, Passive opens and Attempts fail is displayed.	TCP statistics information is displayed.

17.2 Show TCP Connections

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the tcp connections for the switch such as Local IP Address type, Local IP, Local Port and Remote Port. It also displays if a connection is TCP MD5 protected and the number of incoming segments that failed MD5 authentication. show tcp connections	Mode: Privileged EXEC Mode	1	**show tcp connections**	Enter the command. You can check if the tcp connections for the switch such as Local IP Address type, Local IP, Local Port and Remote Port are displayed.	TCP connections for the switch are displayed.

17.3 Show TCP Listeners

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the information such as Local IP Address Type, Local IP and Local Port for each listeners in the network. show tcp listeners	Mode: Privileged EXEC Mode	1	**show tcp listeners**	Enter the command. You can check if the information such as Local IP Address Type, Local IP and Local Port for each listeners in the network is displayed.	The information such as Local IP Address Type, Local IP and Local Port for each listeners in the network is displayed.

17.4 Show TCP Retransmission Details

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the tcp retransmission details. show tcp retransmission details	Mode: Privileged EXEC Mode	1	**show tcp retransmission details**	Enter the command. You can check if the tcp retransmission details are displayed.	The TCP retransmission details are displayed.

18. UDP

18.1 Show UDP Statistics

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the udp statistics such as InDatagrams, outDatagrams, HC InDatagrams, HC OutDatagrams, UDP No Ports and UDP IN Errors. show udp statistics [vrf <vrf-name>]	Mode: Privileged EXEC Mode	1	**show udp statistics**	Enter the command. You can check if the udp statistics such as InDatagrams, outDatagrams, HC InDatagrams, HC OutDatagrams, UDP No Ports and UDP IN Errors are displayed.	The UDP statistics such as InDatagrams, outDatagrams, HC InDatagrams, HC OutDatagrams, UDP No Ports and UDP IN Errors are displayed.

18.2 Show UDP Connections

Command Description	Pre-Conditions	#	Step	Description	Result
This command displays the udp configurations such as Local IP Address Type, Local IP, Local Port, Remote IP Address Type, Remote IP and Remote Port for various connections. show udp connections [vrf <vrf-name>]	Mode: Privileged EXEC Mode	1	**show udp connections**	Enter the command. You can check if the udp configurations such as Local IP Address Type, Local IP, Local Port, Remote IP Address Type, Remote IP and Remote Port for various connections are displayed.	The UDP configurations such as Local IP Address Type, Local IP, Local Port, Remote IP Address Type, Remote IP and Remote Port for various connections are displayed.

Pushing Performance

HARTING Technology Group
info@HARTING.com
www.HARTING.com

Version vom 10. 2013